世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 20/10	A1	(11) 国際公開番号	WO00/05716
		(43) 国際公開日	2000年2月3日(03.02.00)

(21) 国際出願番号 PCT/JP99/03887

(22) 国際出願日 1999年7月21日(21.07.99)

(30) 優先権データ
特願平10/206967 1998年7月22日(22.07.98) JP
特願平10/289831 1998年10月12日(12.10.98) JP

(71) 出願人
松下電器産業株式会社
(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP]
〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)
(72) 発明者
田川健二(TAGAWA, Kenji)
〒576-0021 大阪府交野市妙見坂5丁目5番地305号 Osaka, (JP)
南 賢尚(MINAMI, Masataka)
〒656-2311 兵庫県津名郡東浦町久留麻2349-1 Hyogo, (JP)
小塚雅之(KOZUKA, Masayuki)
〒572-0024 大阪府寝屋川市石津南町19番1-1207号 Osaka, (JP)

(74) 代理人
中島司朗(NAKAJIMA, Shiro)
〒531-0072 大阪府大阪市北区豊崎三丁目2番1号
淀川5番館6F Osaka, (JP)

(81) 指定国 AU, CN, ID, KR, MX, SG, 欧州特許 (DE, FR, GB, IT, NL)

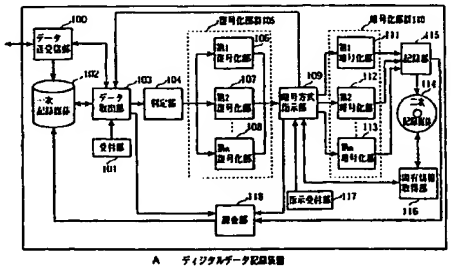
添付公開書類
国際調査報告書

(54)Title: **DIGITAL DATA RECORDING DEVICE AND METHOD FOR PROTECTING COPYRIGHT AND EASILY REPRODUCING ENCRYPTED DIGITAL DATA AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM**

(54)発明の名称 著作権を保護し、記録媒体に記録された暗号化されたディジタルデータの再生を容易にするディジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) Abstract

A data transmitting/receiving unit receives electronically allotted encrypted digital data for recording on a primary recording medium. Digital data use provider-dependent different encryption systems and contain attribute information describing encryption systems. Digital data retrieved at a data retrieving unit is judge for an encryption system at a judging unit and is decoded at one proper decoding unit. An inherent information acquiring unit acquires identification information of a secondary recording medium or a reproducing device depending on whether or not the second recording medium is mountable/demountable to/from the reproducing device. An encryption system instructing unit selects one encrypting unit out of a plurality of encrypting units based on the acquired identification information. The one encrypting unit creates an encryption key based on the identification information and encrypts digital data. A recording unit records digital data on the secondary recording medium, and an accounting unit charges costs according to accounting information described in the attribute information.



A ディジタルデータ記録装置

A ... DIGITAL DATA RECORDING DEVICE
100 ... DATA TRANSMITTING/RECEIVING UNIT
101 ... RECEIVING UNIT
102 ... PRIMARY RECORDING MEDIUM
103 ... DATA RETRIEVING UNIT
104 ... JUDGING UNIT
105 ... DECODING UNIT GROUP
106 ... FIRST DECODING UNIT
107 ... SECOND DECODING UNIT
108 ... Nth DECODING UNIT
109 ... ENCRYPTION SYSTEM INSTRUCTING UNIT
110 ... ENCRYPTING UNIT GROUP
111 ... FIRST ENCRYPTING UNIT
112 ... SECOND ENCRYPTING UNIT
113 ... Nth ENCRYPTING UNIT
114 ... SECONDARY RECORDING MEDIUM
115 ... RECORDING UNIT
116 ... INHERENT INFORMATION ACQUIRING UNIT
117 ... INSTRUCTION RECEIVING UNIT
118 ... ACCOUNTING UNIT

(57)要約

データ送受信部は、電子配信される暗号化されたディジタルデータを受信し、一次記録媒体に記録する。ディジタルデータは、提供者ごとに暗号方式が異なり、暗号形式を記載した属性情報を含んでいる。データ取出部で取り出されたディジタルデータは、判定部で暗号形式が判定され、適切な一の復号化部で復号される。固有情報取得部は、二次記録媒体が再生装置に対して着脱可能か否かで二次記録媒体又は再生装置の識別情報を取得する。暗号方式指示部は、取得された識別情報に従い、複数の暗号化部から一の暗号化部を選ぶ。一の暗号化部は、識別情報を基に暗号鍵を生成し、ディジタルデータを暗号化する。記録部は二次記録媒体にディジタルデータを記録し、課金部は、属性情報に記載された課金情報に従い課金する。

明 細 書

著作権を保護し、記録媒体に記録された暗号化されたディジタルデータの再生を容易にするディジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体

技術分野

本発明は、ディジタルデータの著作権保護を図るディジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体に関する。

背景技術

近年のインターネットの普及により、ＰＣ（パーソナルコンピュータ）を用いて、ホームページ上から好みの音楽データなどをダウンロードにより入手し、クレジットカードなどの決済手段を通じて支払いを行う、いわゆる EC(Electronic Commerce：電子商取引)による音楽流通が広がりつつある。このようなインターネットを通じた EC による音楽流通（以下「電子音楽配信」という。）が普及することは、ユーザがレコード店に行く必要がなくなることを意味し、現在のＣＤ(Compact Disc)中心の音楽流通を大きく変えるものになる可能性を持っている。

ところで、音楽を鑑賞するスタイルという点に注目すると、自宅で鑑賞する以外にも、携帯型の再生装置を用いて、通勤、通学途中に鑑賞する、あるいは車の中で鑑賞するというスタイルもかなりの割合を占める。この場合には、音楽データをＭＤ(Mini Disc)等の可搬型の媒体に記録する必要がある。

また、電子音楽配信においては、各社それぞれ独自の暗号方式を採用し、著作権保護を図っている。すなわち、製作会社、流通経路、利用形態等に応じて、それぞれ異なる暗号方式を採用している。このため、電子音楽配信によって音楽デ

ータをＭＤ等に記録する場合、流通段階での音楽データをそのまま記録したとき、ＭＤ等を再生する再生装置は、各暗号方式に対応して復号化できる装置が求められる。この結果、装置規模が大きくなり、価格の上昇を招き、ユーザにとっては不利益となる。

一方、ユーザの利益だけを考えるなら、電子音楽配信された音楽データの暗号を復号化してＭＤ等に記録するようにすれば、再生装置は、暗号解読を必要としないので安価なものを提供できることになる。

しかしながら、この場合には、不正なコピーを助長して著作権保護を図ることができない。

発明の開示

本発明は、上記課題に鑑みなされたものであり、著作権保護を図り、かつ記録媒体に記録された音楽データを安価なディジタルデータ再生装置で再生することができるディジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体を提供することを目的とする。

上記目的は、ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化ディジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでディジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたディジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたディジタルデータを再暗号化させることで達成できる。

このような構成によって、再生装置で容易に再生できる暗号化部で再暗号化されたディジタルデータを記録媒体に記録することができ、かつ暗号化されている

ので著作権の保護を図ることができる。

ここで、前記記録媒体に記録されたディジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第１暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第２暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第１暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能なときは、前記第２暗号化部によりディジタルデータの暗号化を行わせることができる。

このような構成によって、記録媒体がいずれかの再生装置で再生されるときには、その記録媒体の識別情報を基に生成される暗号鍵でディジタルデータを暗号化し、特定の一の再生装置で再生されるときには、その一の再生装置の識別情報を基に生成される暗号鍵でディジタルデータを暗号化することによって、記録媒体に記録されたディジタルデータを再生装置で再生することができる。

ここで、前記ディジタルデータ記録装置は、更に、前記ディジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

このような構成によって、異なるセキュリティレベルを有する暗号化方式の暗号化部を選択することができ、かつ、暗号化部に応じた料金を支払うことができる。

ここで、前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化ディジタルデータを、前記復号化手段により復号化することを禁止することができる。

このような構成によって、暗号化部で暗号鍵を生成できないときには、ディジタルデータを復号する処理をなくすことができる。

ここで、前記暗号化手段の有する複数の暗号化部による暗号化されたディジタルデータは、前記通信手段により受信されたディジタルデータの暗号化に比べいずれもセキュリティレベルが低いとすることができる。

このような構成によって、再生装置は、ディジタルデータの再生が容易となり、再生装置のコストダウンにつながる。

ここで、前記通信手段により受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたディジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化ディジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化ディジタルデータを復号化するように前記復号化手段を制御することができる。

このよな構成によって、受信されたディジタルデータごとに異なるセキュリティレベルを有する暗号化方式で暗号化されていても、暗号化方式に対応した復号化部を選んで、復号化することができる。

ここで、前記ディジタルデータ記録装置は、更に、前記ディジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、受信した暗号化ディジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

このような構成によって、ディジタルデータの復号化と再暗号化とに対応した利用料金が徴収され、著作権の保護を図ることができる。

また、上記目的は、ディジタルデータを記録媒体に記録するディジタルデータ記録方法において、暗号化されたディジタルデータをディジタルネットワークを

介して受信する通信ステップと、前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたディジタルデータを前記記録媒体に記録する記録ステップとを有することが達成できる。

このような構成によって、再生装置で容易に再生できる暗号化方式で暗号化されたディジタルデータを記録媒体に記録することができ、かつ、暗号化されているので著作権の保護を図ることができる。

ここで、前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することができる。

このような構成によって、通信手段で受信された暗号化されたディジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても、復号化することができる。

また、上記目的は、ディジタルデータを第1記録媒体に記録するディジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたディジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体で達成できる。

このような構成によって、容易に再生できる暗号化方式で暗号化されたディジタルデータを記録媒体に記録し、かつ、著作権の保護を図る機能のないディジタルデータ記録装置に適用して、このような機能を発揮させることができる。

ここで、前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式からいーの暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範囲第１１項に記載のコンピュータ読み取り可能な記録媒体とすることができる。

このような構成によって、通信手段で受信された暗号化されたディジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても復号化することができる。

図面の簡単な説明

図１は、本発明に係るディジタルデータ記録装置の実施の形態１の構成図である。

図２は、上記実施の形態のハード構成を示す外観図及び上記実施の形態で得られた記録媒体の再生装置の外観図である。

図３は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の一例を示す図である。

図４は、上記実施の形態の一次記録媒体にダウンロードされた音楽データのデータ構造の一例を示す図である。

図５は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の他の一例を示す図である。

図６は、上記実施の形態の動作を説明するフローチャートのその１である。

図７は、上記実施の形態の動作を説明するフローチャートのその２である。

図８は、本発明に係るディジタルデータ記録装置の実施の形態２の構成図である。

図９は、上記実施の形態の情報提供者が提供するディジタル信号を記録する際の表示部に表示される情報を示す図である。

図１０は、上記実施の形態の動作を示すフローチャートである。

図１１は、本発明に係るディジタルデータ記録装置の実施の形態３の構成図である。

図１２は、上記実施の形態の情報提供者が提供するディジタル信号の属性情報のデータ構造を示す図である。

図１３は、上記実施の形態の動作を示すフローチャートのその１である。

図１４は、上記実施の形態の動作を示すフローチャートのその２である。

図１５は、本発明に係るディジタルデータ記録装置の実施の形態４の構成図である。

図１６は、本発明に係るディジタルデータ記録装置の実施の形態６の構成図である。

図１７は、上記実施の形態のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図１８は、上記実施の形態の記録媒体に記録される管理情報のデータ構造の一例を示す図である。

図１９は、上記実施の形態の動作を説明するフローチャートである。

図２０は、上記実施の形態で記録された記録媒体を再生するディジタルデータ再生装置の構成図である。

図２１は、上記デジタルデータ再生装置の動作を説明するフローチャートである。

図２２は、本発明に係るディジタルデータ記録装置の実施の形態７の構成図で

ある。

図２３は、上記実施の形態のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図２４は、上記実施の形態の動作を説明するフローチャートである。

図２５は、上記実施の形態７の変形例のディジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

発明を実施するための最良の形態

以下、本発明に係るディジタルデータ記録装置の実施の形態について図面を用いて説明する。

（実施の形態１）

図１は、本発明に係るディジタルデータ記録装置の実施の形態１の構成図である。このディジタルデータ記録装置は、データ送受信部１００と、受付部１０１と、一次記録媒体１０２と、データ取出部１０３と、判定部１０４と、復号化部群１０５と、暗号方式指示部１０９と、暗号化部群１１０と、二次記録媒体１１４と、記録部１１５と、固有情報取得部１１６と、指示受付部１１７と、課金部１１８とを備えている。

なお、このディジタルデータ記録装置の二次記録媒体１１４と記録部１１５以外は、一般には図２に示すようにＰＣ（パーソナルコンピュータ）２０１で実現され、記録部１１５は、例えばＤＶＤ(Digital Versatile Disc)－RAM ドライブ２０２で、二次記録媒体１１４は、ＤＶＤ－RAM ディスク２０３でそれぞれ実現される。

このディジタルデータ記録装置は、インターネットを介して配信される暗号化されたディジタルデータである音楽データを受信し、一次記録媒体１０２にダウンロードした後、復号化部群１０５でディジタルデータを復号化し、暗号化部群１１０で再度暗号化したディジタルデータとして、記録部１１５で二次記録媒体

１１４に記録する。

なお、本実施の形態では、電子音楽配信について説明するけれども、ディジタルデータの種類は、音楽データに限るものではなく、映像データ、文字データあるいはこれらの組み合わせでもよい。

データ送受信部１００は、モデムと制御ソフトで実現される通信部であり、電話回線を通じて情報提供者のホストコンピュータ（図示せず）に接続される。受付部１０１で受け付けられた希望する曲の購入要求をデータ取出部１０３を介して通知されると、ホストコンピュータに送信する。インターネットを介して、ホストコンピュータから購入要求に従い配信される音楽データをダウンロードし、一次記録媒体１０２に記録する。また、曲を購入したときに生じる課金情報をホストコンピュータに送信する。

ここで、情報提供者が提供する情報について説明する。情報提供者は、曲販売のサイト、すなわち自社のホームページを開設しており、曲名、価格などユーザの購入時に必要な情報、あるいは購買意欲をかきたてる情報を提供している。ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。

図３は、情報提供者が提供する情報、すなわち曲販売用のホームページの一例を示すものである。表示される情報としては、曲名３０１、歌手名３０２、収録時間３０３、価格３０４などの内容からなる。ここで、曲名３０１、歌手名３０２は、それぞれ、個々の音楽データの曲名、歌手名を表す情報である。収録時間３０３は、個々の曲の収録時間（再生時間）を示し、価格３０４は、個々の曲の販売価格を示している。これらの情報をもとに、ユーザは受付部１０１を通じて好みの曲を選択し、購入要求を通知することができる。もちろん、情報提供者が提供する情報は、図３に示すように、文字情報に限られるものではなく、ジャケットピクチャのような画像や、試聴用の音楽データであってもよいことは言うまでもない。

受付部１０１は、キーボードやマウス等からなり、ＰＣの表示画面に表示され

た図３に示した情報を見たユーザから音楽データの購入要求を受け付ける。受け付けた曲の購入要求は、データ取出部１０３を介して、データ送受信部１００に通知される。

一次記録媒体１０２は、一般にはＰＣのハードディスク等で実現され、データ送受信部１００で受信された暗号化されたディジタルデータである音楽データを記憶している。また、一次記録媒体のセキュアな領域には、課金部１１８によって、ダウンロードされた音楽データを二次記録媒体１１４に記録したとき、例えば暗号化した課金データが記録される。

図４は、一次記録媒体１０２に記憶されているダウンロードした音楽データ、すなわち情報提供者が提供する音楽データのデータ構造の一例を示すものである。情報提供者が提供する音楽データは、大きく音楽データの曲名や歌手名、価格などの情報である属性情報４０１と、音楽データそのものである曲データ部４０２とから構成される。

属性情報４０１は、ISRC 情報４０３、曲名４０４、歌手名４０５、価格４０６、情報提供者名４０７、暗号形式４０８から構成される。以下、これらの属性情報について説明する。

ISRC(International Standard Recording Code)情報４０３は、音楽データごとに割り当てられる固有の情報であって、国コード（２つの ASCII 文字)、オーナーコード（３つの ASCII 文字)、記録年（数字２桁)、シリアル番号（数字５桁）で構成される。曲名４０４、歌手名４０５は、それぞれ音楽データの曲名、歌手名を表す文字情報である。価格４０６は、音楽データの価格を表す情報である。なお、本実施の形態では、ダウンロードした音楽データをディジタルデータ記録装置を用いて、二次記録媒体に記録したときに請求される金額を示している。

情報提供者名４０７は、音楽データの提供者名、あるいは著作権者名を示す情報である。つまり、ユーザが本ディジタルデータ記録装置を用いて音楽データを記録したときに課金し、その金額をどの業者に振り分ければよいのかを示す情報

である。

暗号形式４０８は、ダウンロードした音楽データがどの暗号形式で暗号化されているかを示す情報である。すなわち音楽データは、情報提供者ごとに異なる暗号方式で暗号化されている。例えば、情報提供者Ａ、情報提供者Ｂ、情報提供者Ｃが音楽データを提供する場合、情報提供者Ａの提供する音楽データはＡ方式で暗号化されており、情報提供者Ｂの提供する音楽データはＢ方式で暗号化されており、情報提供者Ｃの提供する音楽データはＣ方式で暗号化されている。なお、本実施の形態では、情報提供者の提供する情報が、さまざまな形式で暗号化されている場合に、それを記録した二次記録媒体１１４を再生装置で著作権の保護を図りつつ、容易に解読できる暗号形式に変換することが発明の主たる目的であり、暗号化のアルゴリズムの詳細な説明については省略する。

また、属性情報４０１においては、価格４０６、情報提供者名４０７は改竄されると情報提供者が不利益を被るおそれがあるため、必要に応じて暗号化されている。

データ取出部１０３は、暗号方式指示部１０９からディジタルデータの取り出し指示を受けると、一次記録媒体１０２から、まず属性情報４０１を取り出し、属性情報４０１を課金部１１８に通知する。また、属性情報４０１中の暗号形式４０８の情報は、判定部１０４に通知する。なお、属性情報４０１中、価格４０６等が暗号化されているときは、復号化部群１０５によって、復号化してから課金部１１８に通知する。さらに一次記録媒体１０２から曲データ部４０２を取り出し、判定部１０４に出力する。データ取出部１０３で取り出されたデータは、すでに述べたように、情報提供者ごとに異なる暗号方式で暗号化されている。

判定部１０４は、データ取出部１０３から通知された暗号形式４０８の情報に基づいて、復号化部群１０５のいずれの復号化部に音楽データを出力するか判定する。

復号化部群１０５は、ｎ個の復号化部よりなり、第１復号化部１０６はＡ方

式で暗号化されたディジタルデータを復号し、第２復号化部１０７はＢ方式で暗号化されたディジタルデータを復号し、第ｎ復号化部１０８はＮ方式で暗号化されたディジタルデータを復号する。各復号化部１０６～１０８は、情報提供者ごとの復号モジュールからなっている。

例えば、判定部１０４に通知された暗号形式４０８の情報がＢ方式であれば、判定部１０４は、音楽データの曲データ部４０２のディジタルデータを第２復号化部１０７に出力し、復号する。第２復号化部１０７は、入力されたディジタルデータを復号して、暗号方式指示部１０９に出力する。

第１から第ｎ復号化部１０６～１０８のいずれかにより暗号化されたデータを復号する際、復号鍵が必要であればデータ送受信部１００でデータの暗号方式に応じた復号鍵を入手し、データを復号化する。このようにして情報提供者ごとに異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化する。

暗号方式指示部１０９は、指示受付部１１７から暗号方式の種類の指示を受けているときは、その指示に従った固有情報の取得を固有情報取得部１１６に指示する。固有情報取得部１１６から指示した固有情報の通知を受けたときは、データ取出部１０３に音楽データの取り出しを指示する。固有情報取得部１１６から指示に従った固有情報を取得できない旨の通知を受けたときには、表示部（図示せず）に指示された暗号方式の種類では暗号化できない旨を表示させる。また、指示受付部１１７から暗号方式の種類の指示を受けていないときには、固有情報取得部１１６に二次記録媒体１１４の属性に従った固有情報の取得を指示する。固有情報取得部１１６から固有情報又は固有情報を取得できない旨を通知されると、データ取出部１０３に音楽データの取り出しを指示する。固有情報を取得できない旨の通知を受けたときには、乱数を発生する。

暗号方式指示部１０９は、指示受付部１１７から暗号方式の指示を受け付けているときは、その指示に応じた一の暗号化部を選び、復号化部群１０５のいずれ

かの復号化部１０６、１０７、…、１０８から復号されたディジタルデータの入力を受けると、固有情報取得部１１６から通知された固有情報とともに、復号されたディジタルデータを通知する。

また、暗号方式指示部１０９は、指示受付部１１７から指示を受け付けていないときには、固有情報取得部１１６から通知された固有情報の種類に従い、一の暗号化部を選び、復号化部群１０５のいずれかの復号化部１０６～１０８から復号されたディジタルデータの入力を受けると、固有情報とともにディジタルデータを通知する。固有情報取得部１１６から固有情報を取得できない旨の通知を受けているとき、発生させた乱数とともに、一の暗号化部にディジタルデータを通知する。

暗号化部群１１０は、ｎ個の暗号化部１１１、１１２、…、１１３からなる。各暗号化部１１１、１１２、…、１１３は、異なる種類の暗号鍵によって、通知されたディジタルデータを暗号化する。例えば、第１暗号化部１１１は、二次記録媒体１１４の固有の識別情報を基に作成される暗号鍵で暗号化する。第２暗号化部１１２は、二次記録媒体１１４を再生する再生装置（図示せず）の固有の識別情報を基に作成される暗号鍵で暗号化する。第ｎ暗号化部１１３は、乱数を基に作成される暗号鍵で暗号化する。暗号化部１１１～１１３で用いられる各暗号鍵のデータサイズは、一次記録媒体１０２に記憶されている暗号化されたディジタルデータの暗号鍵のデータサイズよりも小さく設定される。

二次記録媒体１１４に記録される暗号化されたディジタルデータの暗号鍵のデータサイズが小さいことは、このディジタルデータを解読する際の困難性が低いことを意味する。したがって、二次記録媒体１１４を再生する再生装置でのディジタルデータの復号化に要する構成が簡単化されることになり、再生装置のコスト減につながる。

例えば、指示受付部１１７からの指示がないときに、暗号方式指示部１０９が固有情報取得部１１６から二次記録媒体の識別情報の通知を受けているときには、

第１暗号化部１１１に二次記録媒体の識別情報を通知する。第１暗号化部１１１は、その識別情報を基に暗号鍵を作成し、暗号方式指示部１０９から通知された音楽データの属性情報４０１の暗号形式４０８を書き換えるとともに、曲データ部４０２を、生成した暗号鍵で暗号化する。暗号化したディジタルデータを記録部１１５に通知する。

また、暗号方式指示部１０９は、指示受付部１１７から二次記録媒体１１４を再生する再生装置（図示せず）の固有情報による暗号化の指示を受けると、固有情報取得部１１６に再生装置の固有の識別情報を取得するよう指示する。固有情報取得部１１６から再生装置の固有の識別情報を通知されると、その識別情報と復号化部群１０５から通知された復号されたディジタルデータとを第２暗号化部１１２に通知する。

第２暗号化部１１２は、暗号方式指示部１０９から通知された識別情報を基に暗号鍵を生成し、生成した暗号鍵でディジタルデータを暗号化して記録部１１５に通知する。この際、音楽データの属性情報４０１の暗号形式４０８の内容を書き換えるのは、指示受付部１１７から指示を受け付けないときと同様である。

二次記録媒体１１４は、例えば図２に示した DVD-RAM ディスク、ＭＤ、再生装置（図示せず）の機種により埋め込み型あるいは取り外し可能な型の小型の半導体メモリ等からなり、暗号化部群１１０で暗号化された音楽データが記録部１１５によって記録される。例えば、DVD-RAM ディスク２０３にディジタルデータが記録されていれば、図２に示すように、DVD-Audio プレーヤ２０４に DVD-RAM ディスク２０３を挿入して音楽を聴取することができる。

記録部１１５は、例えば、図２に示した DVD-RAM ドライブ２０２で実現され、暗号化部群１１０から通知されたディジタルデータを二次記録媒体１１４に記録する。また、記録が終了すると、その旨、課金部１１８に通知する。

固有情報取得部１１６は、暗号方式指示部１０９から二次記録媒体１１４の固有の識別情報の取得を指示されたときには、例えば、DVD-RAM の場合は

BCA(Burst Cutting Area)に書かれている情報を読み出し、通知する。なお、この二次記録媒体１１４の固有の識別情報は、媒体ごとにユニークであり、通常ディスクの製造時に記録される情報であって、ユーザの通常の操作では読み出されたり、書き換えることができない。

したがって、この識別情報を基に暗号鍵を生成して、この暗号鍵で暗号化されたディジタルデータが DVD-RAM ディスクに記録されるので、万一悪意を持ったユーザがビットコピー可能なツールを用いて DVD-RAM ディスクの内容を複製し、再生しようとしても、復号鍵の基になる情報が異なるため、正常に復号化することができない。この結果、音楽データの著作権を確実に保護することができる。

また、暗号方式指示部１０９から二次記録媒体１１４が装着された再生装置（図示せず）の固有の識別情報の取得を指示されたときには、固有情報取得部１１６は、再生装置の識別情報を読み出し、暗号方式指示部１０９に通知する。この再生装置の固有の識別情報も再生装置の製造時に付される装置ごとのユニークな識別情報であるので、ユーザの通常の操作では読み出されたり、書き換えられたりすることはできない。したがって、この識別情報を基に暗号化された場合も、特定の再生装置でしか再生することができない。

なお、固有情報取得部１１６は、暗号方式指示部１０９から指示された固有の識別情報を取得できないとき、即ち、二次記録媒体１１４又は再生装置に識別情報が付されていない場合には、指示された種類の固有の識別情報を取得できない旨を暗号方式指示部１０９に通知する。

固有情報取得部１１６は、暗号方式指示部１０９から固有情報の種類の指示を受けずに、固有情報の取得の指示を受けると、二次記録媒体１１４が DVD-RAM ディスクなどの再生装置から取り外し可能なものであるか、それとも、小型の半導体メモリのような再生装置に埋め込まれた取り外し不可能ものであるかを判断し、取り外し可能なものであれば、その二次記録媒体１１４の固有の識別

情報を読み出し、暗号方式指示部１０９に二次記録媒体１１４の識別情報を通知し、取り外し不可能なものであれば、再生装置の識別情報を読み出し、同様に再生装置の識別情報を通知する。識別情報を取得できないときは、その旨を暗号方式指示部１０９に通知する。

指示受付部１１７は、ＰＣのキーボードやマウスで実現され、ユーザから暗号方式の種類の指示を受け付け、暗号方式指示部１０９に通知する。

先に述べた図３に示すホームページの情報では、販売価格は１通りしかなかったけれども、図５に示すようなホームページの内容であれば、価格（１）５０１、価格（２）５０２の２通りの販売価格が示されている。

価格（１）５０１は、二次記録媒体１１４の固有の識別情報を基にディジタルデータを暗号化して記録するときの価格を示しており、価格（２）５０２は、二次記録媒体１１４を再生する再生装置の固有の識別情報を基にディジタルデータを暗号化して記録するときの価格を示している。なお、これらの２種類の価格は、情報提供者側でそれぞれ個別に自由に設定可能である。

ユーザは、指示受付部１１７から二次記録媒体１１４の利用形態に応じて、図５に示す曲情報あるいはその価格情報を参照して好みの暗号形態でディジタルデータを暗号化することを指示することができる。例えば、特定の再生装置でのみ再生するとき、即ち、他の再生装置で二次記録媒体１１４を再生しないときには、再生装置の固有の識別情報を基に暗号化することを指示する。図５に示すように再生装置の識別情報を基に暗号化するほうが、価格（２）５０２に示すように一般的に安価である。これは、他の再生装置で再生することができないので、二次記録媒体１１４の固有の識別情報を基に暗号化するよりも自由度が低いからである。ユーザは、自由に再生装置を選んで再生したいときには、二次記録媒体１１４の識別情報を基に暗号化するよう指示すればよい。

なお、指示受付部１１７と上述の受付部１０１とは、一体として構成されているけれども、説明上、２つの構成要素として説明した。

課金部１１８は、データ取出部１０３から音楽データの属性情報４０１の通知を受け、記憶している。記録部１１５から暗号化されたディジタルデータを二次記録媒体１１４に記録した旨の通知を受けると、属性情報中の価格４０６を参照して課金額を決定し、一次記録媒体１０２のセキュアな領域に属性情報４０１とともに課金情報として書き込む。

なお、価格４０６が図５に示したように価格（１）５０１、価格（２）５０２のように複数あるときは、暗号方式指示部１０９から通知された第１から第ｎ暗号化部１１１～１１３のいずれが利用されたかに従い課金額を決定する。

次に、本実施の形態の動作を図６、図７のフローチャートを用いて説明する。

先ず、受付部１０１はユーザからのホームページ表示の要求を受け、データ送受信部１００が音楽データを提供する情報提供者が開設するホームページにアクセスし、データ取出部１０３によって表示部（図性せず）にホームページ（図３、図５参照）を表示させる（Ｓ６０２）。

次に、データ取出部１０３は、受付部１０１からユーザの希望する音楽データの購入指示を待ち、指定された音楽データの配信を受けるようデータ送受信部１００に指示する（Ｓ６０４）。データ送受信部１００は、音楽データを受信すると、一次記録媒体１０２にダウンロードする（Ｓ６０６）。

ユーザは、ホームページの表示をみて、暗号方式の種類を二次記録媒体１１４の利用形態に応じて、指示受付部１１７から入力する。

暗号方式指示部１０９は、指示受付部１１７から暗号方式の種類の指示を通知されたか否か判断し（Ｓ６０８）、通知されたときは、指示された暗号方式の種類に用いる固有情報の取得を固有情報取得部１１６に指示する（Ｓ６１０）。固有情報取得部１１６から指示された固有情報を取得できない旨の通知を受けたか否かを判断し（Ｓ６１２）、その旨の通知を受けたときは、指示された暗号方式の種類では暗号化できない旨を表示部（図示せず）に表示させ（Ｓ６１４）、処理を終了する。指示した種類の固有情報の通知を受けたときには、データ取出部

１０３にディジタルデータの取り出しを指示する。

データ取出部１０３は、一次記録媒体１０２に記録されている音楽データを取り出す（Ｓ６１６）。

Ｓ６０８において、暗号方式指示部１０９は、指示受付部１１７から指示を通知されないと判断したとき、固有情報取得部１１６に固有情報の種類を指定しないで、固有情報の取得を指示する（Ｓ６１８）。

固有情報取得部１１６は、二次記録媒体１１４の属性（再生装置（図示せず）に装着された二次記録媒体１１４が取り外し可能か不可能か）を判断し、取り外し可能な二次記録媒体１１４のときは二次記録媒体１１４の識別情報を取得し、取り外し不可能な二次記録媒体１１４のときは再生装置の識別情報を取得する（Ｓ６２０）。

暗号方式指示部１０９は、固有情報取得部１１６から取得された固有（識別）情報又は、固有情報を取得できなかったときはその旨の通知を受けると（Ｓ６２２）、データ取出部１０３にディジタルデータの取り出しを指示し、Ｓ６１６に移る。

次に、判定部１０４は、データ取出部１０３で取り出された音楽データの属性情報４０１中の暗号形式４０８を参照して、復号化部群１０５のいずれの復号化部１０６～１０８で復号するかを判定する（Ｓ７０２）。

判定部１０４で判定された一の復号化部は、判定部１０４を介して入力されたディジタルデータを復号化し、復号したディジタルデータを暗号方式指示部１０９に出力する（Ｓ７０４）。

暗号方式指示部１０９は、既に固有情報取得部１１６から通知されている固有情報（取得できない旨の情報も含む）に従い、暗号化部群１１０の一の暗号化部を選び、固有情報（取得できない旨の情報に対しては発生した乱数）と復号化されたディジタルデータとを通知する（Ｓ７０６）。

暗号方式指示部１０９から通知を受けた一の暗号化部は、固有（識別）情報に

基づいて暗号鍵を生成し（乱数の通知に対しては乱数に基づいて暗号鍵を生成し）、ディジタルデータを暗号化する。この際、属性情報４０１のうち暗号形式４０８の内容も書き換えられる（Ｓ７０８）。

記録部１１５は、第１～第ｎ暗号化部１１１～１１３のいずれかから通知されたディジタルデータを二次記録媒体１１４に記録し（Ｓ７１０）、記録が終了すると課金部１１８に通知する。

課金部１１８は、記録部１１５から通知を受けると、データ取出部１０３から通知されている価格４０６等に従い課金額を決定し、課金情報を一次記録媒体１０２に記録して（Ｓ７１２）処理を終了する。

上記実施の形態では、復号化部群１０５は、情報提供者ごとの復号モジュール（復号化部）からなるものとしたけれども、復号化部群は、音楽データの品質、例えば２４ビットのＬＰＣＭ(Liner Pulse Code Modulation)、ＭＰ３(Moving Picture Experts Group 1 Audio Layer 3)等のディジタルデータ、に応じて各復号化部を設けてもよい。高品質の２４ビットのＬＰＣＭは、解読の困難性の高い暗号化されたディジタルデータとし、通常品質のＭＰ３は解読の困難性の低い暗号化されたディジタルデータとしておき、第１復号化部は２４ビットのＬＰＣＭのディジタルデータを復号し、第２復号化部はＭＰ３のディジタルデータを復号するようにしてもよい。

上記実施の形態では、暗号化部群１１０は、固有情報の種類で各暗号化部を設けたけれども、上述した品質に対応して、第１復号化部で復号化されたディジタルデータは第１暗号化部で暗号化し、第２復号化部で復号化されたディジタルデータは第２暗号化部で暗号化し、第ｎ復号化部で復号化されたディジタルデータは第ｎ暗号化部で暗号化するようにしてもよい。この場合、第１暗号化部で暗号化に用いる暗号鍵のデータサイズは、第２暗号化部のそれよりも大きく、第２暗号化部のそれは第ｎ暗号化部のそれよりも大きく設定する。そして、課金部は、ディジタルデータの復号化がされた復号化部と復号化されたディジタルデータを

再暗号化部がされた暗号化部とによって課金額を決定する。このようにすることによって、高品質の音楽データの方がより著作権の保護を確実なものとすることができる。また、この際、価格についても情報提供者は高品質の音楽データに高価格を設定することができる。

なお、上記実施の形態のディジタルデータ記録装置は、図１にその構成図を示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないディジタルデータ記録装置に摘要して著作権の保護機能を有する装置とすることができる。

また、本実施の形態では、ディジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらず音楽データ、あるいは、属性情報のみをいったんユーザのＰＣ内の一次記録媒体１０２に記録しておき、一次記録媒体１０２に記録されているディジタルデータに対して購入手続きを行う形態も考えられる。

また、本実施の形態では、属性情報４０１は曲データ４０２と別個に記述するとして説明を行ったが、いわゆるWater Mark（電子すかし）の形式で曲データ４０２のディジタルデータ中に埋め込むことも可能である。

また、本実施の形態において、復号化部群１０５と暗号化部群１１０との間の暗号方式指示部１０９を介してのデータ入出力に関しては特に言及はしていないが、セキュリティ上、認証を行ってデータを送信するか、あるいは復号化部群１０５、暗号方式指示部１０９及び暗号化部群１１０を１つのチップで実現する、といった方法で復号化されたデータの漏洩を防ぐようにしてもよい。

また、課金情報を記録するときには、一次記録媒体１０２中のセキュアな領域に記録するとして説明を行ったが、課金情報に関しては、一次記録媒体１０２とは別のＩＣカードなどの記録媒体を設け、これに記録することが可能である。

本実施の形態では、課金のタイミングについては、説明を省略したが、例えば、

ディジタルデータを二次記録媒体１１４に記録するときに必ずホストコンピュータと接続していなければいけないとするか、課金額が一定の金額に達するとホストコンピュータに自動的に接続するか、あるいは、課金情報記録後、一定の日時が経過すると自動的にホストコンピュータに接続する、としてもよい。

更に、本実施の形態では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報との組み合わせたものなどでもよいことはもちろんである。

（実施の形態２）

図８は、本発明に係わるディジタルデータ記録装置の実施の形態２の構成図である。このディジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部２１０１、一次記録媒体２１０２、データ取出部２１０３、暗号方式判定部２１０４、第１の復号化部２１０５、第２の復号化部２１０６、第３の復号化部２１０７、暗号化部２１０８、記録部２１０９、二次記録媒体２１１０、入力部２１１１、表示部２１１２、記録媒体固有情報取得部２１１３を備える。また、復号化部群２１１５は、第１の復号化部２１０５、第２の復号化部２１０６、第３の復号化部２１０７から構成されるが、復号化部は３つに限るものではなく、ここでは、複数の復号化部から構成されることを示している。

なお、本実施の形態では、以後、記録対象となるデータを音楽データであるとし、音楽データはインターネットを通じて配信されるものとする。また、情報提供者ごとに異なる暗号方式でデータを暗号化しているものとする。

情報提供者は、曲名、価格、コピー制御情報など（以後、属性情報と称する）購入時に必要な情報、あるいは購買意欲をかきたてる情報をを音楽データに重畳または音楽データから分離して提供するものとするが、本実施の形態では、属性情報を音楽データから分離して提供する形態について説明する。

データ送受信部２１０１は、モデムで実現される通信部であり、電話回線を通

じて提供者のホストコンピュータ（図示せず）に接続される。まず、ユーザは情報提供者が提供する属性情報を取得する。データ送受信部２１０１により取得した属性情報は、一次記録媒体２１０２に記録され、その一部または全部が表示部２１１２に表示される。図９は、表示部２１１２に表示される情報の一例を示すものである。表示される情報としては、曲名２２０１、曲名コード２２０２、歌手名２２０３、データ入手先２２０４などの内容からなる。ここで、曲名２２０１、歌手名２２０３は、それぞれ音楽データに対する曲名、歌手名を表す情報である。曲名コード２２０２は、音楽データを他の音楽データと識別するための識別子であり、例えばＩＳＲＣ（International Standard Recording Code）情報が付される。これらの情報をもとに、ユーザは入力部２１１１を通じて好みの曲を選択し、購入要求を通知することができる。データ入手先２２０４は、本実施の形態では該当する曲が記録されているＵＲＬ（Uniform Resource Locator）情報とする。もちろん、曲名コード２２０２にＩＳＲＣ情報が付されていれば、曲名コード２２０２からデータ入手先を特定することも可能である。

入力部２１１１は、マウス、キーボード等から実現され、ユーザからの曲の購入の指示、すなわち記録指示を受け付け、データ送受信部２１０１に通知する。ユーザは表示部２１１２に表示された情報を元に、マウスでその曲名等をクリックして音楽データの記録を指示する。

入力部２１１１から音楽データの記録指示があると、データ送受信部２１０１から電話回線を通じて提供者のホストコンピュータから記録要求のあった曲をダウンロードする。この際に、属性情報中のＵＲＬ情報をもとに曲データの位置を特定する。ダウンロードされたデータはいったん一次記録媒体２１０２に記録される。

一次記録媒体２１０２は、一般にはパソコンのハードディスクであって、ユーザが購入を希望した音楽データを暗号化されたまま記録する。したがって以後の動作に関しては、必ずしも常に提供者のホストコンピュータと接続している必要

はない。

データ取出部２１０３は、一次記録媒体２１０２から記録対象となる音楽データを取り出す。このとき、ユーザは表示部２１１２に表示される図９に示した情報と同程度の情報をもとに、二次記録媒体２１１０へ記録する音楽データを入力部２１１１を通じて選択する。データ取出部２１０３で取り出されたデータは、各情報提供者ごとの暗号方式で暗号化されている。このため、適当な復号方式で復号することを暗号方式判定部２１０４により判定する。具体的には、ディジタルデータのヘッダ部に暗号方式を識別できる情報を付加して送信する、属性情報に暗号方式を記述しておく、などの方法が考えられ、これらの値に応じて暗号方式を判定する。

第１の復号化部２１０５、第２の復号化部２１０６、第３の復号化部２１０７は、各情報提供者ごとの復号方式が存在していることを示すものであって、必ずしも３つに限られるわけではない。暗号方式判定部２１０４により適当な復号化部を選択し、復号化部により暗号化されたデータを復号する。このとき、例えば暗号方式判定部２１０４で取得したデータの暗号方式に応じた復号鍵を入手または生成し、復号化部はこの復号鍵をもとにデータを復号化する。したがって、異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化することになる。

次に、暗号化部２１０８にて復号化されたデータの暗号化を行うが、ここでは、記録媒体固有の固有情報を暗号鍵情報として暗号化を行うこととする。なお、記録媒体固有情報をもとに暗号化を行う一の方法については、特開平５－２５７８１６公報に開示されているので、ここでは詳しい説明は省略する。

記録媒体固有情報取得部２１１３は、暗号化部２１０８からの指示に従い、二次記録媒体２１１０から固有情報を取り出し、暗号化部２１０８へ伝達する。

暗号化部２１０８は、記録媒体固有情報取得部２１１３で取得した固有情報を暗号鍵として、暗号化する。

ここで、二次記録媒体２１１０固有の情報について説明する。

二次記録媒体２１１０は、媒体ごとの固有の識別情報を持っている。これは例えばＤＶＤ－ＲＡＭ（Digital Versatile Disc Random Access Memory）の場合、ＢＣＡ（Burst Cutting Area）に書かれた情報に相当する。この情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持ったユーザがビットコピー可能なツールを用いてディスクの内容を複製したとしても、復号鍵のもとになる情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

記録部２１０９は、暗号化されたデータを二次記録媒体２１１０に記録する。

以上のように構成されたディジタルデータ記録装置について、以後図１０のフローチャートを用いてその動作を説明する。

まず、データ送受信部２１０１は、属性情報をダウンロードし（Ｓ２３０１）、ユーザからのディジタルデータの記録指示を待ち（Ｓ２３０２）、指示されたディジタルデータをダウンロードし、一次記録媒体２１０２に記録する（Ｓ２３０３）。次に、ダウンロードしたデータの暗号方式を判定し、適当な復号化部２１０５～２１０７へ復号化を指示する（Ｓ２３０４）。復号化部２１０５～２１０７により復号化する（Ｓ２３０５）。暗号化部２１０８は、復号化されたデータが入力されると、記録媒体固有情報取得部２１１３から二次記録媒体２１１０の固有情報を取得する（Ｓ２３０６）。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部２１０８はデータを暗号化する（Ｓ２３０７）。記録部２１０９は、暗号化されたデータを二次記録媒体２１１０に記録し（Ｓ２３０８）、処理を終了する。

以上で、本発明の実施の形態２のディジタルデータ記録装置に関する説明を終わる。

次に、本発明の実施の形態３のディジタルデータ記録装置に関する説明を行う。

（実施の形態３）

図１１は、本発明に係わるディジタルデータ記録装置の実施の形態３の構成図である。このディジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部２１０１、一次記録媒体２１０２、データ取出部２１０３、暗号方式判定部２１０４、復号化部群２１１５、属性情報取得部２４０１、コピー制御情報検出判定部２４０２、コピー制御情報変換部２４０３、課金情報算出部２４０４、暗号化部２１０８、記録部２１０９、二次記録媒体２１１０、入力部２１１１、表示部２１１２、記録媒体固有情報取得部２１１３を備える。

なお、実施の形態３では、実施の形態２のディジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

まず、本実施の形態において、記録対象となるデータの属性情報が図１２の通りであるとする。図１２に示す属性情報は、図９に示す属性情報に加えて、コピー制御情報２５０１、課金情報２５０２等の情報がある。ここで、コピー制御情報２５０１は、コピーが許可されている世代数、あるいは回数の情報からなる。例えば世代数に関しては、「無制限にコピー可」、「１世代だけコピー可（孫コピー禁止）」、「コピー禁止」等の値を取る。一方、回数に関しては、コピー許可されている回数のことで、０以上の整数値を取りうる。例えば「孫コピー不可」は、二次記録媒体２１１０にディジタルデータを記録後、二次記録媒体２１１０中のデータをもとにコピーすることを許可しないことを意味する。「無制限に許可」は、特に制限しないことを意味する。「２回コピー可」など、コピーの回数の情報が含まれる場合は、二次記録媒体２１１０に記録できる回数を意味する。

属性情報取得部２４０１は、一次記録媒体２１０２から、再生すべきデータに対応する属性情報を取得する。ここでは、コピー制御情報と課金情報を取り出す。なお、属性情報は著作権保護情報や課金情報を含むので、一次記録媒体２１０２中のセキュアな領域に記録して、ユーザの通常の操作ではアクセスできないこと

が望ましい。

コピー制御情報検出判定部２４０２は、属性情報中のコピー制御情報を取り出し、以後のコピーが許可されているかどうか、許可されているとすればその世代数、あるいは回数の情報を取得する。

コピー制御情報検出判定部２４０３は、コピーが許可されている場合、コピー制御情報を必要に応じて書き換える。例えば、孫コピーが禁止されているときは、コピー制御情報の値を以後のコピーを禁止するように変更し、コピー許可回数が制限されているときは、許可回数から「１」減じた値に変更する。

ここで重要となるのは、コピー許可回数が設定されているとき、一般に、一次記録媒体２１０２に記録されたデータを何回二次記録媒体２１１０にコピーさせるかという数値であるため、コピー制御情報の書き換え対象となるのは、一次記録媒体２１０２中に記録されているデータである。したがって、一次記録媒体２１０２中に記録されている。コピー許可回数を「１」減じた値に変換し、二次記録媒体２１１０に記録すべきコピー許可回数は０として記録する。

課金情報算出部２４０４は、属性情報取得部２４０１で取得した属性情報から該当する曲の課金情報を取得し、これをもとに課金額を算出し、一次記録媒体２１０２中のセキュアな領域に記録する。

以上のように構成されたディジタルデータ記録装置について、以下、図１３および図１４のフローチャートを用いてその動作を説明する。

まず、データ送受信部２１０１は、属性情報をダウンロードし（Ｓ２６０１）、ユーザからのディジタルデータの記録指示を待ち（Ｓ２６０２）、指示されたディジタルデータをダウンロードし、一次記録媒体２１０２に記録する（Ｓ２６０３）。次に、記録対象となるデータの属性情報を属性情報取得部２４０１により取得する（Ｓ２６０４）。コピー制御情報判定部２４０２により属性情報中のコピー制御情報を判定し、コピーが許可されているかどうかを判定する（Ｓ２６０５）。コピーが許可されているときは、コピーが許可されている世代、回数の情

報を取得し、必要に応じてコピー制御情報変換部２４０３で書き換える（Ｓ２６０６）。コピーが許可されていない場合は、以後の処理を中断する（Ｓ２６０７）。次に暗号方式を判定し、復号化群２１１５中の適当な復号化部へ復号化を指示する（Ｓ２６０８）。復号化部２１０５～２１０７により復号化を行う（Ｓ２６０９）。復号化が終わると、属性情報取得部２４０１で取得した属性情報中の課金情報から適切な課金額を算出する（Ｓ２６１０）。

暗号化部２１０８は、復号化されたデータが入力されると、記録媒体固有情報取得部２１１３から二次記録媒体２１１０の固有情報を取得する（Ｓ２６１１）。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部２１０８はデータを暗号化する（Ｓ２６１２）。記録部２１０９は、暗号化されたデータを二次記録媒体２１１０に記録し（Ｓ２６１３）、処理を終了する。

以上で、本発明の実施の形態３に関する説明を終わる。

（実施の形態４）

次に、本発明に係わるディジタルデータ記録装置の実施の形態４について説明する。このディジタルデータ記録装置は、実施の形態２とほぼ同一であるが、固有情報取得送出部２８０３、記録部２１０９、二次記録媒体２１１０が第２のディジタルデータ記録装置内にある点と、暗号鍵の情報のみが異なる。図１５は、本発明に係わるディジタルデータ記録装置の実施の形態４の構成図である。このディジタルデータ記録装置は、第１のディジタルデータ記録装置２８００と、第２のディジタルデータ記録装置２８０１とからなる。

第１のディジタルデータ記録装置２８００は、データ送受信部２１０１、一次記録媒体２１０２、データ取出部２１０３、暗号方式判定部２１０４、復号化部群２１１５、暗号化部２１０８、入力部２１１１、表示部２１１２、固有情報取得部２８０２備える。

第２のディジタルデータ記録装置２８０１は、固有情報取得送出部２８０３、記録部２１０９、二次記録媒体２１１０を備える。

なお、実施の形態４では、実施の形態２のディジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

暗号化部２１０８へ復号化部群２１１５にて復号されたデータが入力されると、記録媒体固有情報取得部２８０２は、第２のディジタルデータ記録装置２８０１中の固有情報取得送出部２８０３へ固有情報の送出要求を出す。固有情報取得送出部２８０３は、第２のディジタルデータ記録装置２８０１に装着されている二次記録媒体２１１０の固有識別情報、あるいは第２のディジタルデータ記録装置２８０１固有の識別情報、あるいはその両方を取得し、固有情報取得部８０２へ送出する。

暗号化部２１０８では、第２のディジタルデータ記録装置２８０１に装着されている二次記録媒体１１０の固有識別情報、あるいは第２のディジタルデータ記録装置８０１固有の識別情報、あるいは、二次記録媒体２１１０の固有識別情報と第２のディジタルデータ記録装置２８０１固有の識別情報の組み合わせの情報を暗号鍵の一部としてデータを暗号化し、第２のディジタルデータ記録装置２８０１へ出力する。第２のディジタルデータ記録装置２８０１中の記録部２１０９は暗号化されたデータを二次記録媒体２１１０へ記録する。

なお、固有情報取得送出部２８０３で取得送出する固有情報であるが、二次記録媒体２１１０が第２のディジタルデータ記録装置２８０１に固定的に設けられているときは、装置固有の識別情報とし、二次記録媒体２１１０が着脱自在に設けられているときは、二次記録媒体２１１０固有の固有情報、あるいは二次記録媒体２１１０の固有識別情報と第２のディジタルデータ記録装置２８０１固有の識別情報の組み合わせの情報とすることにより、より柔軟な暗号方式を使用することが可能になる。

以上で、実施の形態４の説明を終わる。

（実施の形態５）

次に、本発明に係わるディジタルデータ記録装置の実施の形態５について説明する。このディジタルデータ記録装置は、実施の形態２、３および４とほぼ同一である。ここでは、実施の形態４の説明に用いた構成図、図１５を用いて説明する。相違点は、二次記録媒体２１１０に応じた暗号形式を採用し、記録することである。つまり、DVD-RAMと半導体メモリとでは取り扱うデータの最小単位、暗号化データを書きこむデータ量の単位の単位が異なるため、固有情報取得部２８０２は、固有情報取得送出部２８０３から、媒体の情報も取得して、最適なデータの単位で暗号化を行なうことになる。このため、暗号化部２１０８が複数存在し、適切な暗号化部へ固有情報ならびに媒体情報も伝達するものである。以上より、DVD-RAM に限らず、半導体メモリ、ＩＣカード、ハードディスク等を二次記録媒体２１１０として使用することが可能となる。

以上で、実施の形態５の説明を終わる。

なお、上記実施の形態２～５は現状において最善の効果が期待できるシステム例として説明したにすぎない。本発明は、その要旨を逸脱しない範囲で実施変更することができる。具体的には以下に示すような変更実施が可能である。

また、実施の形態２～５では、ディジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらずいったんユーザのＰＣ内の一次記録媒体２１０２に記録しておき、一次記録媒体２１０２に記録されているディジタルデータに対して購入手続きを行う形態も考えられる。

また、実施の形態２～５では、コピー制御情報を属性情報に記述するとして説明を行なったが、いわゆるＷａｔｅｒ Ｍａｒｋ（電子すかし）の形式でディジタルデータ中に埋め込むことも可能である。

また、課金情報を記録するときには、一次記録媒体２１０２中のセキュアな領域に記録するとして説明を行なったが、課金情報に関しては、一次記録媒体２１０２とは別のＩＣカードなどの記録媒体を設け、これに記録することが可能であ

る。

また、実施の形態２～５では、情報提供者が提供する情報を音声情報として説明したが、これに限るものでなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報の組み合わせたものなどでもよいことはもちろんである。

（実施の形態６）

図１６は、本発明に係るディジタルデータ記録装置の実施の形態６の構成図である。

このディジタルデータ記録装置は、通信部３１０１と、記録媒体３１０２と、受信データ記録判定部３１０３と、表示部３１０４と、入力操作部３１０５と、記録媒体固有情報取得部３１０６と、暗号化部３１０７と、記録部３１０８と、課金情報記録部３１０９と、課金情報記録媒体３１１０と、課金部３１１１とを備えており、ＰＣで実現される。

通信部３１０１は、モデムで実現され、電話回線を介してデータ提供者のホストコンピュータ（図示せず）及び課金センタ（図示せず）に接続される。ホストコンピュータからディジタルデータとその属性情報とを受信すると、受信データ記録判定部３１０３に通知する。

また、通信部３１０１は、課金センタから利用料の問い合わせがあると、その旨課金部３１１１に通知し、課金部３１１１から課金情報の通知を受けると、電話回線を介して、課金センタに課金情報を通知する。

本実施の形態では、データ提供者が提供するディジタルデータを音楽データであるとして説明する。データ提供者は、提供する音楽データを必要に応じて暗号化したディジタルデータとし、ディジタルデータには、情報識別子が付されている。情報識別子は、曲名コードであり、他の音楽と識別するためのものである。

また、ディジタルデータには、属性情報が付加されている。属性情報は、ディジタルデータの利用料金等を示すものであり、どの情報提供者から提供された情

報であるかを示す情報も含まれている。

図１７は、属性情報の内容の一例を示す図である。属性情報３２０１には、ディジタルデータの曲名３２０２、演奏者（歌手）３２０３、曲名コード３２０４、記録料金３２０５、１回あたりの再生料金３２０６、再生可能回数３２０７、暗号状態３２０８、コピー許可３２０９等の項目の内容が含まれる。

ここで、曲名３２０２、演奏者３２０３は、表示部３１０４に表示して、ユーザがコピー（複製）をするか否かを指示する判断資料となるものである。曲名コード３２０４は、音楽データを他の音楽データと識別するための識別子であり、曲ごとにユニークなものであり、例えばＩＳＲＣ（International Standard Recording Code）が付される。なお、このコードは国コード（２つのＡＳＣＩＩ文字）、オーナーコード（３つのＡＳＣＩＩ文字）、記録年（数字２桁）、シリアル番号（数字５桁）で構成されている。

記録料金３２０５、１回あたり再生料金３２０６、再生可能回数３２０７等は、課金基準データを構成し、いずれもその音楽データの利用料金を算定する為の情報である。

記録料金３２０５は、通信部３１０１で受信されたディジタルデータを記録媒体３１０２に記録する際の料金である。１回あたりの再生料金３２０６は、記録媒体３１０２に記録されたディジタルデータの再生１回あたりの料金を示している。再生可能回数３２０７は、記録媒体３１０２に記録されたディジタルデータの再生が許容される回数を示している。「１００回」と記録されているときには、１００回に限り再生できることを示している。また、再生回数が一定回数以上になると、その後の料金が不要となる買い取り形式の設定も可能である。

暗号状態３２０８は、暗号有無フラグであり、通信部３１０１で受信されたディジタルデータが暗号化されているか否かを示すものである。

コピー許可３２０９は、記録許可フラグであり、ユーザ側で記録する、即ち、記録媒体３１０２に受信された音楽データを記録することを許可するか否かを示

す情報である。「１回のみ可」とは、１度だけ記録することが許可され、「許可」は、何度でも記録することが許可されていることを示している。

なお、本発明は、受信された音楽データを記録媒体３１０２に記録（複製）し、再生するときの音楽の著作権保護を図ることを主目的としたものであるので、この音楽データをリアルタイムに聴取するだけが許可されている場合についての説明は、簡単にする。この場合は、コピー許可３２０９は、「不可」とされている。このディジタルデータ記録装置には、復号化部と出力部とがその構成から省略されているけれども、通信部３１０１で受信されたディジタルデータは復号化部で復号され、出力部から音楽が出力される。この際、課金基準データには、聴取料金が含まれている。

記録媒体３１０２は、書き換え可能な記憶部材からなり、装置本体に着脱可能に取り着けられており、例えば、ＤＶＤ-RAM 等で構成される。

記録媒体３１０２の書き換え不能なセキュアな領域には、記録媒体３１０２の固有情報が予め記録されている。

また、記録媒体３１０２には、記録部３１０８によって、暗号化部３１０７で暗号化されたディジタルデータが記録される。

更に、記録媒体３１０２には、記録されたディジタルデータの管理情報と属性情報とが記録部３１０８によって記録されている。

受信データ記録判定部３１０３は、通信部３１０１からディジタルデータとその属性情報３２０１との通知を受けると、その属性情報３２０１を最初に通知されたとき記憶し、属性情報のうち、曲名３２０２、演奏者３２０３、記録料金３２０５、１回あたり再生料金３２０６等を表示部３１０４に表示させ、ディジタルデータを暗号化部３１０７に通知する。

入力操作部３１０５からコピー（複製）指示を受けると、指示された音楽の曲名コード３２０４のディジタルデータのコピーが可能か否かを属性情報３２０１のコピー許可３２０９を見て判断する。コピーが許可であれば、記録媒体固有情

報取得部３１０６に記録媒体３１０２の固有情報を取得するよう指示する。また、暗号化部３１０７に曲名コード３２０４と暗号状態３２０８を通知する。

コピーが不可であれば、表示部３１０４にその旨を表示させる。

受信データ記録判定部３１０３は、記録部３１０８からコピー終了の通知を受けると、記憶している属性情報３２０１の項目、コピー許可３２０９を書き換える。即ち、コピー許可３２０９が「１回のみ」とされているときには「コピー不可」に、「何回のみ可」と数字が記録されているときには「１」を減じた数字にそれぞれ書き換える。なお、この属性情報３２０１を記憶する記憶領域は、ＥＥＰＲＯＭ内に設けられており、このディジタルデータ記録装置の電源がオフされた場合でも記憶内容は消失されない。

例えば、暗号化部３１０７に曲名コード３２０４の「song01」を通知した後に、記録部３１０８からコピー終了の通知を受けると、「song01」に対応する項目、コピー許可３２０９を「１回のみ可」から「コピー不可」に書き換える。このようにすることによってデータ提供者の有する権利が侵されることを防止できる。

表示部３１０４は、液晶ディスプレイやＣＲＴ等からなり、受信データ記録判定部３１０３の制御により、ディジタルデータである音楽データの曲名等の表示や、コピーができない旨の表示をする。

入力操作部３１０５は、マウス等からなり、ユーザのコピー指示を受け付け、受信データ記録判定部３１０３に通知する。ユーザは、表示部３１０４に表示された曲名や演奏者の表示を見て、記録媒体３１０２にその音楽をダウンロードしようとするとき、マウスでその曲名等をクリックして、その音楽のコピーを指示する。

記録媒体固有情報取得部３１０６は、受信データ記録判定部３１０３から固有情報の取得指示を受けると、記録媒体３１０２のセキュアな領域に記録されている固有情報を読み出し、暗号化部３１０７に通知する。

暗号化部３１０７は、記録媒体固有情報取得部３１０６から通知された固有情報を基に暗号鍵を作成する。受信データ記録判定部３１０３から通知されたディジタルデータを作成した暗号鍵を用いて暗号化したディジタルデータを作成し、記録部３１０８に通知する。

なお、受信データ記録判定部３１０３から通知されたディジタルデータが暗号化されている旨の通知を受けている場合には、そのディジタルデータを復号化しておいてもよいし、そのままの状態でもよい。

例えば、記録媒体３１０２に記録すべきディジタルデータ dataAを受信データ記録判定部３１０３から通知された場合に、記録媒体３１０２の固有情報を基に暗号鍵ＫＭを作成すると、暗号化したディジタルデータＥ（KM,dataA）を作成する。他の記録媒体にディジタルデータ dataAを記録する場合には、その他の記録媒体の固有情報を基に暗号鍵 K'M を作成したときは、暗号化したディジタルデータＥは、Ｅ（K'M,dataA）となる。

ここで、ディジタルデータの暗号化の技術については、特開平５－２５７８１６号公報に記載されている。

記録部３１０８は、暗号化部３１０７から通知された暗号化されたディジタルデータを記録媒体３１０２に記録する。この際、記録媒体３１０２に記録したディジタルデータの管理情報を作成して、記録媒体３１０２に記録する。

図１８は、管理情報の一例を示す図である。管理情報３３０１には、記録したディジタルデータの識別子である曲名コード３２０４と、記録媒体３１０２に記録されたディジタルデータの記録開始アドレス３３０２、記録終了アドレス３３０３とが対応して記録される。

記録媒体３１０２に記録されたディジタルデータを再生する際、この管理情報３３０１が参照される。

また、記録部３１０８は、記録媒体３１０２に暗号化されたディジタルデータ及び管理情報の記録が終了すると、受信データ記録判定部３１０３に記憶されて

いる記録したディジタルデータに対応する属性情報３２０１を読み出し、記録媒体３１０２に書き込む。更に、受信データ記録判定部３１０３にコピー終了の通知をする。また、課金情報記録部３１０９に、記録したディジタルデータの曲名コードを通知する。

課金情報記録部３１０９は、記録部３１０８から曲名コード３２０４の通知を受けると、受信データ記録判定部３１０３に記憶されている曲名コード３２０４に対応する属性情報３２０１の記録料金３２０５を読み出し、記録料金が有料のときは、課金情報記録媒体３１１０にその曲名コードと記録料金と記録日時等を課金情報として記録する。

課金情報記録媒体３１１０は、ＲＡＭカード等からなり、記録媒体３１０２にダウンロードしたディジタルデータの課金情報が課金情報記録部３１０９によって記録される。

課金部３１１１は、通信部３１０１を介して課金センタ（図示せず）からの利用料の問い合わせがあると、課金情報記録媒体３１１０に記録されている未決済の課金情報を読み出し、通信部３１０１に通知する。通知が終了すると、課金センタに通知済（決済）のフラグを課金情報記録媒体３１１０に記録する。

次に、本実施の形態の動作を図１９のフローチャートを用いて説明する。

先ず、受信データ記録判定部３１０３は、ユーザからディジタルデータの記録指示を待ち（Ｓ３４０２）、指示されたディジタルデータのコピーが許可されているか否かを属性情報２０１を見て判断する（Ｓ３４０４）。否のときは、コピーが許可されていない旨を表示部３１０４に表示させ（Ｓ３４０６）、処理を終了する。

コピーが許可されているときは、記録媒体固有情報取得部３１０６は、記録媒体３１０２のセキュアな領域に記録されている記録媒体３１０２の固有情報を取得し、暗号化部３１０７に通知する（Ｓ３４０８）。

暗号化部３１０７は、固有情報を基に暗号鍵を作成し、ディジタルデータを暗

号化する（Ｓ３４１０）。

記録部３１０８は、暗号化されたディジタルデータを記録媒体３１０２に記録する（Ｓ３４１２）。

次に、課金情報記録部３１０９は、記録されたディジタルデータの記録料金が有料か否かを判断する（Ｓ３４１４）。無料であれば、処理を終了し、有料であれば、課金情報記録媒体１１０に課金情報を記録して（Ｓ３４１６）、処理を終了する。

図２０は、上述のディジタルデータ記録装置で記録媒体３１０２に記録されたディジタルデータの再生装置の構成図である。

このディジタルデータ再生装置は、記録媒体３１０２と、入力操作部３５０１と、再生情報読出部３５０２と、表示部３５０３と、記録媒体固有情報取得部３５０４と、復号化部３５０５と、再生部３５０６と、課金情報記録部３５０７と、課金情報記録媒体３５０８とを備えている。

記録媒体３１０２は、上記ディジタルデータ記録装置で暗号化されたディジタルデータと管理情報３３０１と属性情報３２０１とが記録されたＤＶＤ-ＲＡＭを識別する識別子である固有情報が記録されている。

入力操作部３５０１は、ユーザから再生開始の指示を受けると、再生情報読出部３５０２に初期起動の指示を与える。ユーザから曲名の指示を受けると、その曲名を再生情報読出部３５０２に通知する。なお、初期起動の指示の他に記録媒体３１０２がこのディジタルデータ再生装置に挿入されたときにも自動再生モードの指示が再生情報読出部３５０２に与えられる。

再生情報読出部３５０２は、入力操作部３５０１から初期起動の指示を受けると、記録媒体３１０２に記録されている属性情報３２０１を読み出し、その項目である曲名３２０２及び演奏者３２０３の一覧を表示部３５０３に表示させる。

また、入力操作部３５０１から曲名の指示又は、自動再生モードの指示を受けると、属性情報３２０１の対応する再生可能回数３２０７が「１」以上であるか

否かを判断する。再生可能回数３２０７が「１」以上であれば、その曲名コード３２０４を読み出し、管理情報３３０１の記録開始アドレスから記録終了アドレスまでに記録された暗号化されたディジタルデータを読み出し、復号化部３５０５に通知する。この際、記録媒体固有情報取得部３５０４に固有情報を取得するよう指示するとともに、課金情報記録部３５０７に、曲名コード３２０４と１回あたりの再生料金３２０６とを通知する。更にディジタルデータの読み出しが終了すると、属性情報３２０１の項目である再生可能回数３２０７の数を「１」減じた数に書き換える。なお、再生可能回数３２０７が「無限」の場合には、そのままにする。

再生情報読出部３５０２は、再生可能回数が「１」未満であると判断したとき、表示部３５０３に再生可能回数が越えた旨を表示させる。

表示部３５０３は、液晶ディスプレイ等からなり、再生情報読出部３５０２で読み出された曲名等を一覧表示する。また、再生可能回数を超えてのユーザからの曲名指定に対して、再生可能回数が越えた旨を表示する。

記録媒体固有情報取得部３５０４は、再生情報読出部３５０２から固有情報の取得を指示されると、記録媒体３１０２のセキュアな領域から記録媒体３１０２の識別子である固有情報を取得し、復号化部３５０５に通知する。

復号化部３５０５は、記録媒体固有情報取得部３５０４から固有情報の通知と、再生情報読出部３５０２から暗号化されたディジタルデータの通知とを受けると、固有情報を基に復号鍵を作成して、暗号化されたディジタルデータを復号し、復号化したディジタルデータを再生部３５０６に通知する。

再生部３５０６は、復号化部３５０５からディジタルデータの通知を受けると、デコードして音楽を再生する。音楽の再生を終了すると課金情報記録部３５０７に再生終了を通知する。

課金情報記録部３５０７は、再生部３５０６から再生終了の通知を受けると、再生情報読出部３５０２から通知されている曲名コード３２０４と１回あたりの

再生料金３２０６と再生日時とを課金情報として課金情報記録媒体３５０８に記録する。なお、１回あたりの再生料金３２０６が有料でなければ、記録はしない。

課金情報記録媒体３５０８は、ＲＡＭカード等からなり、課金情報を課金情報記録部３５０７によって記録される。

次に、このディジタルデータ再生装置の動作を図２１に示すフローチャートを用いて説明する。

先ず、ユーザは、再生開始を入力操作部３５０１のリモコン等を用いて指示し、表示部３５０３に表示された曲名を指定する。再生情報読出部３５０２は、音楽の再生要求であるとし（Ｓ３６０２）、指定された曲名の再生可能回数が「１」以上であるか否かを属性情報３２０１をみて判断する（Ｓ３６０４）。再生可能回数が「１」未満であれば、表示部３５０３に再生可能回数を超えた旨を表示させ（Ｓ３６０６）、処理を終了する。

再生可能回数が「１」以上の場合には、再生情報読出部３５０２は、記録媒体３１０２から暗号化されたディジタルデータを読み出し、復号化部３５０５に通知する（Ｓ３６０８）。

記録媒体固有情報取得部３５０４は、記録媒体３１０２から固有情報を取得して復号化部３５０５に通知する（Ｓ３６１０）。

復号化部３５０５は、固有情報を復号鍵として暗号化されたディジタルデータを復号化する（Ｓ３６１２）。

再生部３５０６は、ディジタルデータをデコードして音楽を再生出力する（Ｓ３６１４）。

課金情報記録部３５０７は、再生料金が有料であるか否かを判断し（Ｓ３６１６）、無料のときは何もせずに、有料のときは、課金情報を課金情報記録媒体３５０８に記録して（Ｓ３６１８）、処理を終了する。

（実施の形態７）

図２２は、本発明に係るディジタルデータ記録装置の実施の形態７の構成図で

ある。このディジタルデータ記録装置は、第１ディジタルデータ記録装置３７００と第２ディジタルデータ記録再生装置３７１０とからなる。

第１ディジタルデータ記録装置３７００は、第１記録媒体３７０１と、通信部３１０１と、受信データ１次記録判定部３７０２と、表示部３１０４と、入力操作部３１０５と、１次記録部３７０３と、受信データ読出判定部３７０４と、固有情報取得部３７０５と、暗号化部３７０６と、課金情報記録部３１０９と、課金情報記録媒体３１１０と、課金部３１１１とを備えており、ＰＣで実現される。

第２ディジタルデータ記録再生装置３７１０は、固有情報取得送出部３７０７と、２次記録部３７０８と、第２記録媒体３７０９と、入力操作部３５０１と、再生情報読出部３５０２と、表示部３５０３と、復号化部３５０５と、再生部３５０６と、課金情報記録部３５０７と、課金情報記録媒体３５０８とを備えている。

なお、上記実施の形態６のディジタルデータ記録装置及びディジタルデータ再生装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分についてのみ説明する。

先ず、第１ディジタルデータ記録装置３７００について説明する。上記実施の形態６のディジタルデータ記録装置と異なるのは、第１記録媒体３７０１が本装置に固定的に設けられ、この第１記録媒体３７０１に記録されたディジタルデータが２次記録のために暗号化されて出力されることである。

第１記録媒体３７０１は、本装置３７００内に固定的に設けられたハードディスク等の書き込み可能な記録部材からなる。第１記録媒体３７０１には、通信部３１０１で受信された音楽データであるディジタルデータとその管理情報とが１次記録部３７０３によって書き込まれる。

受信データ１次記録判定部３７０２は、通信部３１０１で受信されたディジタルデータに付された属性データをＥＥＰＲＯＭ内に設けられた記憶領域に書き込む。本実施の形態で受信される属性情報の一例を図２３に示す。属性情報３８０

１は、上記実施の形態６の属性情報３２０１と２次記録料金３８０２が記録されていることと、コピー許可（１次）３８０３と（２次）３８０４との記録の許可回数が示されていることとが異なる。

また、曲名コード「song05」の「曲Ｅ」では、コピーが１次、２次ともに不許可であり、リアルタイムの聴取のみが許可された音楽であることを示している。

受信データ１次記録判定部３７０２は、ユーザからある音楽の２次記録の指示を受けると、先ず１次記録が許可されているか否かを属性情報３８０１の項目コピー許可（１次）３８０３を見て判断する。許可されていないときは、表示部３１０４に不許可である旨を表示させる。許可されているときは、指示された音楽のディジタルデータを１次記録部３７０３に通知する。他の機能は、上記実施の形態６の受信データ記録判定部３１０３と同様である。

１次記録部３７０３は、通知されたディジタルデータを第１記録媒体３７０１に記録する。この際、管理情報を書き込むのは、上記実施の形態６の記録部３１０８と同様である。なお、上記実施の形態６では、記録媒体３１０２の固有情報を基に暗号鍵が作成され、ディジタルデータが暗号化されていたけれども、本実施の形態では、第１記録媒体３７０１が取外され、他の装置で利用されることがないので暗号化されない。

また、１次記録部３７０３は、第１記録媒体３７０１へのディジタルデータの記録が終了すると、受信データ読出判定部３７０４に記録した曲名コード３８０５を通知する。

受信データ読出判定部３７０４は、１次記録部３７０３から曲名コード３８０５の通知を受けると、その音楽の２次記録が許可されているか否かを、受信データ１次記録判定部３７０２の属性情報３８０１中のコピー許可（２次）３８０４を見て判断する。許可されていないとき、又は、許可回数が「１」以上でないときには、表示部３１０４に２次記録が許可されていない旨を表示させる。

受信データ読出判定部３７０４は、２次記録が許可されているときには、管理

情報（図１８参照）を見て、第１記録媒体３７０１に記録されている通知された曲名コードのディジタルデータを読み出して暗号化部３７０６に通知するとともに、固有情報取得部３７０５に固有情報を取得するよう指示する。

また、受信データ読出判定部３７０４は、ディジタルデータの読み出しが完了すると、受信データ１次記録判定部３７０２に記憶されている属性情報３８０１のコピー許可（２次）３８０４の回数から「１」減じた数に書き換える。例えば「１回のみ可」であれば「不許可」に書き換え、「許可」だけであれば、回数に制限がないので、そのまま書き換えは行わない。

なお、受信データ読出判定部３７０４は、暗号化部３７０６にディジタルデータの通知の後に、受信データ１次記録判定部３７０２に記憶されている属性情報を読み出して通知する。

固有情報取得部３７０５は、受信データ読出判定部３７０４から固有情報を取得するよう指示されると、第１ディジタルデータ記録装置３７００に接続されている第２ディジタルデータ記録再生装置３７１０の固有情報取得送出部３７０７に、固有情報の送出を要求する。固有情報取得送出部３７０７から固有情報の通知を受けると、暗号化部３７０６に固有情報を通知する。

暗号化部３７０６は、固有情報取得部３７０５から通知された固有情報を基に暗号鍵を作成し、受信データ読出判定部３７０４から通知されたディジタルデータを暗号化して第２ディジタルデータ記録再生装置３７１０の２次記録部３７０８に送出する。この暗号化されたディジタルデータの送出の後に、通知された属性情報も送出する。

次に、第２ディジタルデータ記録再生装置３７１０について説明する。この第２ディジタルデータ記録再生装置３７１０は、携帯型の例えばヘッドフォンステレオタイプの装置で実現される。また、第２記録媒体３７０９がこの装置３７１０から着脱自在の半導体メモリのＩＣカード等から構成されている。

固有情報取得送出部３７０７は、第１ディジタルデータ記録装置３７００の固

有情報取得部３７０５から固有情報の送出要求を受けると、第２記録媒体３７０９に予め記録されている第２記録媒体固有の媒体識別情報と、この装置３７１０固有の機器識別情報とを取得して、固有情報取得部３７０５に通知する。また、再生情報読出部３５０２から固有情報の通知指示を受けると、復号化部３５０５に媒体識別情報と機器識別情報とを通知する。

２次記録部３７０８は、第１ディジタルデータ記録装置３７００の暗号化部３７０６から暗号化されたディジタルデータと、属性情報との出力を受けると、第２記録媒体３７０９に記録する。併せて、図１８に示したような管理情報３３０１を記録する。復号化部３５０５は、固有情報取得送出部３７０７から通知された媒体識別情報と機器識別情報との２つの情報を基に復号鍵を作成して、再生情報読出部３５０２から通知された暗号化されたディジタルデータを復号する。なお、その他の構成は、上記実施の形態６のディジタルデータ再生装置の構成とほぼ同様である。

次に、第２記録媒体３７０９がこの装置３７１０に固定的に設けられたＩＣカード等から構成される場合について述べる。この場合には、第２記録媒体３７０９がこの装置３７１０以外で再生されることがないことから固有情報取得送出部３７０７は、媒体識別情報を取得することなく、自ら記憶している機器識別情報を固有情報取得部３７０５に通知する。また、復号化部３５０５にも、機器識別情報を通知する。

このように、第２ディジタルデータ記録再生装置３７１０に設けられた第２記録媒体３７０９が着脱自在であるか否かによって、ディジタルデータの暗号化の暗号鍵の作成を媒体識別情報と機器識別情報との組合せによるか、機器識別情報だけで行うかを使い分けることができる。このように使い分けることによっても、ディジタルデータの不正な複製や不正な再生利用を防止することができる。

次に、本実施の形態の動作を図２４に示すフローチャートを用いて説明する。先ず、受信データ１次記録判定部３７０２は、入力操作部３１０５からディジタ

ルデータの２次記録の指示が有るのを待ち（Ｓ３９０２）、ディジタルデータの１次記録が許可されているか否かを属性情報３８０１を見て判断する（Ｓ３９０４）。許可されていないときは、その旨を表示部３１０４に表示させて（Ｓ３９０６）、処理を終了する。

許可されているときは、受信データ１次記録判定部３７０２は、ディジタルデータを１次記録部３７０３に通知する。１次記録部３７０３は、第１記録媒体３７０１にディジタルデータと管理情報とを記録する（Ｓ３９０８）。

次に、課金情報記録部３１０９は、１次記録に対して課金されているか否かを判断し（Ｓ３９１０）、１次コピーが有料の時は課金情報を課金情報記録媒体３１１０に記録する（Ｓ３９１２）。

次に、受信データ読出判定部３７０４は、第１記録媒体３７０１に記録されたディジタルデータの２次記録が許可されているか否かを受信データ１次記録判定部３７０２に記憶されている属性情報３８０１を見て判断する（Ｓ３９１４）。許可されていないときは、２次記録が許可されていない旨を表示部３１０４に表示させ（Ｓ３９１６）、処理を終了する。

許可されているときは、受信データ読出判定部３７０４は、第１記録媒体３７０１からディジタルデータを読み出し、暗号化部３７０６に通知するとともに、固有情報取得部３７０５に第２ディジタルデータ記録再生装置３７１０から固有情報を取得するよう指示する。固有情報取得部３７０５は、固有情報を取得し、暗号化部３７０６に通知する（Ｓ３９１８）。暗号化部３７０６は、通知された固有情報を基に暗号鍵を作成し（Ｓ３９２０）、通知されているディジタルデータを暗号化して第２ディジタルデータ記録再生装置３７１０の２次記録部３７０８に出力する。

２次記録部３７０８は、通知された暗号化されたディジタルデータと属性情報と管理情報とを第２記録媒体３７０９に記録する（Ｓ３９２２）。

また、課金情報記録部３１０９は、２次記録に対して課金されているか否かを判

断し（Ｓ３９２４）、２次記録が有料のときは、課金情報を課金情報記録媒体１１０に記録し（Ｓ３９２６）、処理を終了する。

なお、第２ディジタルデータ記録再生装置３７１０でのディジタルデータの再生動作は、実施の形態６のディジタルデータ再生装置の動作とほぼ同様であるので説明を省略する。

（変形例）

上記実施の形態７では、第２記録媒体３７０９が着脱自在であるときには、第２ディジタル記録再生装置３７１０の機器識別情報と、第２記録媒体３７０９の媒体識別情報とを組合せた暗号鍵でディジタルデータが暗号化されたけれども、本変形例では、暗号化の形態（媒体識別情報のみに基づいた暗号鍵とするのか媒体識別情報に機器識別情報を組合わせた暗号鍵とするのか）をユーザに指定させ、ユーザの利用形態の自由度を拡大している。即ち、第２ディジタルデータ記録再生装置３７１０で第２記録媒体３７０９に記録された音楽を再生しようとするときには、媒体識別情報及び機器識別情報でディジタルデータを暗号化して記録するようにし、他のディジタルデータ再生装置（媒体識別情報を復号鍵として暗号化されたディジタルデータを復号化できる装置）で第２記録媒体３７０９に記録された音楽を再生しようとするときには、媒体識別情報でディジタルデータを暗号化して記録するようにする。ユーザの利用形態に応じて暗号化の形態を選択できるようにしている。

一方、このユーザの利用の自由度に応じて２次記録料金を設定して、著作権の保護を図っている。

以下、本変形例の具体的構成を説明する。なお、本変形例は、図２２に示した第１ディジタルデータ記録装置３７００の構成に若干の機能を追加するものであるので、実施の形態７の構成図をそのまま利用して、本変形例固有の構成についてのみ説明する。

図２５は、受信データ１次記録判定部３７０２に記憶されている属性情報３１

００１の一部を示している。この属性情報３１００１では、図２３に示した属性情報３８０１の２次記録料金３８０２と２次記録料金３１００２との内容が異なる。

２次記録料金３１００２は、暗号化の暗号鍵が媒体識別情報（媒体ＩＤ）３１００３、機器識別情報（機器ＩＤ）３１００４、媒体識別情報と機器識別情報との組合わせ３１００５のいずれであるかによって異なっている。媒体識別情報３１００３を基に暗号鍵が作成されたものでは、他の装置に第２記録媒体３７０９を装着して音楽を再生でき、ユーザの自由度が増すことから２次記録料金（２次複製利用料金）が機器識別情報３１００４又は媒体識別情報と機器識別情報との組合わせ３１００５を基に暗号鍵が作成されたものよりも高額に設定される。ユーザの利用形態の拡大に応じて複製利用料金を課金できるようにしたものである。

固有情報取得部３７０５は、固有情報取得送出部３７０７から機器識別情報と媒体識別情報との通知を受けると、表示部３１０４に第２記録媒体３７０９を他の装置で利用するか、第２ディジタルデータ記録再生装置３７１０でのみ利用するかを表示させ、ユーザの選択を待つ。

ユーザは、入力操作部３１０５より、他の装置を用いるか、第２ディジタルデータ記録再生装置３７１０のみを用いるかを指定する。即ち、暗号鍵を媒体識別情報だけで作成するか、媒体識別情報と機器識別情報との組合わせで作成するかを指示する。

入力操作部３１０５は、この指定を固有情報取得部３７０５と受信データ１次記録判定部３７０２とに通知する。

受信データ１次記録判定部３７０２は、入力操作部３１０５から他の装置を用いるとの通知を受けると、課金情報記録部３１０９に媒体識別情報３１００３を暗号鍵とする２次記録料金である旨を、第２ディジタルデータ記録再生装置のみを用いるとの通知を受けると、媒体識別情報と機器識別情報との組合わせ３１００５を暗号鍵とする２次記録料金である旨を通知する。

固有情報取得部３７０５は、入力操作部３１０５から、他の装置を用いる旨の通知を受けると、暗号化部３７０６に媒体識別情報のみを通知する。また、第２ディジタルデータ記録再生装置３７１０でのみ用いる旨の通知を受けると、同様に媒体識別情報と機器識別情報とを通知する。

課金情報記録部３１０９は、暗号化部３７０６から暗号化されたディジタルデータを２次記録部３７０８に送出した旨の通知を受けると、受信データ１次記録判定部３７０２から通知されている属性情報３１００１の２次記録料金３１００２を見て、課金情報記録媒体３１１０に課金情報を記録する。

なお、本変形例において、第２記録媒体が着脱自在の DVD-RAM であるときには、上記実施の形態６と同様、DVD-RAM 固有の識別情報のみを基に暗号鍵を作成し、ディジタルデータを暗号化して記録するようにできるのは勿論である。

また、本変形例の動作は、上記実施の形態７の動作と基本的に異なるところがないのでその説明は省略する。

なお、上記実施の形態６、７及び変形例において、課金情報記録媒体３１１０、３５０８は例えばＩＣカードにより実現し、ディジタルデータの記録や再生時にＩＣカードをセットしなければ動作しないとすることも可能である。

また、上記実施の形態６、７及び変形例では、通信部３１１０で受信されるディジタルデータが音楽データであるとして説明したけれども、これに限ることはなく、映像データ、音声データ、文字データやこれらの組合せであってもよいのは勿論である。

上記実施の形態６と実施の形態７と変形例のディジタルデータ記録装置及び再生装置並びにディジタルデータ記録再生装置は、図１６、図２０及び図２２にその構成図を示したけれども、各構成要素の機能を発揮するプログラムをコンピュータ読取可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないディジタルデータ記録再生装置に適用して著作権の保護機能を有する装置とすることができる。

産業上の利用可能性

以上のように、本発明に係るディジタルデータ記録装置は、著作権保護を図り、再生装置の低コスト化を実現でき、種々の方式で暗号化されて電子配信されるディジタルデータの記録装置として有用であり、特に電子音楽配信される音楽データの記録装置として最適である。

請求の範囲

1．ディジタルデータを記録媒体に記録するディジタルデータ記録装置において、

暗号化されたディジタルデータをディジタルネットワークを介して受信する通信手段と、

前記通信手段により受信された暗号化ディジタルデータを復号する復号化手段と、

複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでディジタルデータを暗号化する暗号化手段と、

前記暗号化手段により暗号化されたディジタルデータを前記記録媒体に記録する記録手段と、

前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、

前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたディジタルデータを再暗号化させることを特徴とするディジタルデータ記録装置。

2．前記記録媒体に記録されたディジタルデータは、再生装置により再生され、

前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第１暗号化部と、

前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第２暗号化部とを有し、

前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第１暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能なときは、前記第２暗号化部によりディジタルデータの暗号化を行わせることを特徴とする

請求の範囲第１項に記載のディジタルデータ記録装置。

３．前記ディジタルデータ記録装置は、更に、

前記ディジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第１項に記載のディジタルデータ記録装置。

４．前記記録媒体に記録されたディジタルデータは、再生装置により再生され、

前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第１暗号化部と、

前記再生装置の識別情報を基に生成した暗号鍵によりディジタルデータを暗号化する第２暗号化部とを有し、

前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第１暗号化部によりディジタルデータの暗号化を行わせ、着脱不可能なときは、前記第２暗号化部によりディジタルデータの暗号化を行わせることを特徴とする請求の範囲第３項に記載のディジタルデータ記録装置。

５．前記制御手段は、

前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化ディジタルデータを、前記復号化手段により復号化することを禁止することを特徴とする請求の範囲第４項に記載のディジタルデータ記録装置。

６．前記暗号化手段の有する複数の暗号化部による暗号化されたディジタルデー

タは、前記通信手段により受信されたディジタルデータの暗号化に比べいずれもセキュリティレベルが低いことを特徴とする請求の範囲第 1 項記載のディジタルデータ記録装置。

7．前記通信手段により受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、

前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたディジタルデータをそれぞれ復号化し、

前記制御手段は、前記通信手段により受信された暗号化ディジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化ディジタルデータを復号化するように前記復号化手段を制御することを特徴とする請求の範囲第1項に記載のディジタルデータ記録装置。

8．前記ディジタルデータ記録装置は、更に、

前記ディジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、受信した暗号化ディジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第7項に記載のディジタルデータ記録装置。

9．ディジタルデータを記録媒体に記録するディジタルデータ記録方法において、

暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたディジタルデータを前記記録媒体に記録する記録ステップとを有することを特徴とするディジタルデータ記録方法。

１０．前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるディジタルデータは当該ディジタルデータの暗号化方式を示す属性情報を含み、

複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することを特徴とする請求の範囲第９項に記載のディジタルデータ記録方法。

１１．ディジタルデータを第１記録媒体に記録するディジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、

暗号化されたディジタルデータをディジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化ディジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたディジタルデータを暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたディジタルデータを前記第１記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラム

を記録したコンピュータ読み取り可能な記録媒体。

１２．前記通信ステップにより受信されるディジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、

複数の暗号化方式からいーの暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたディジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範囲第１１項に記載のコンピュータ読み取り可能な記録媒体。

図1

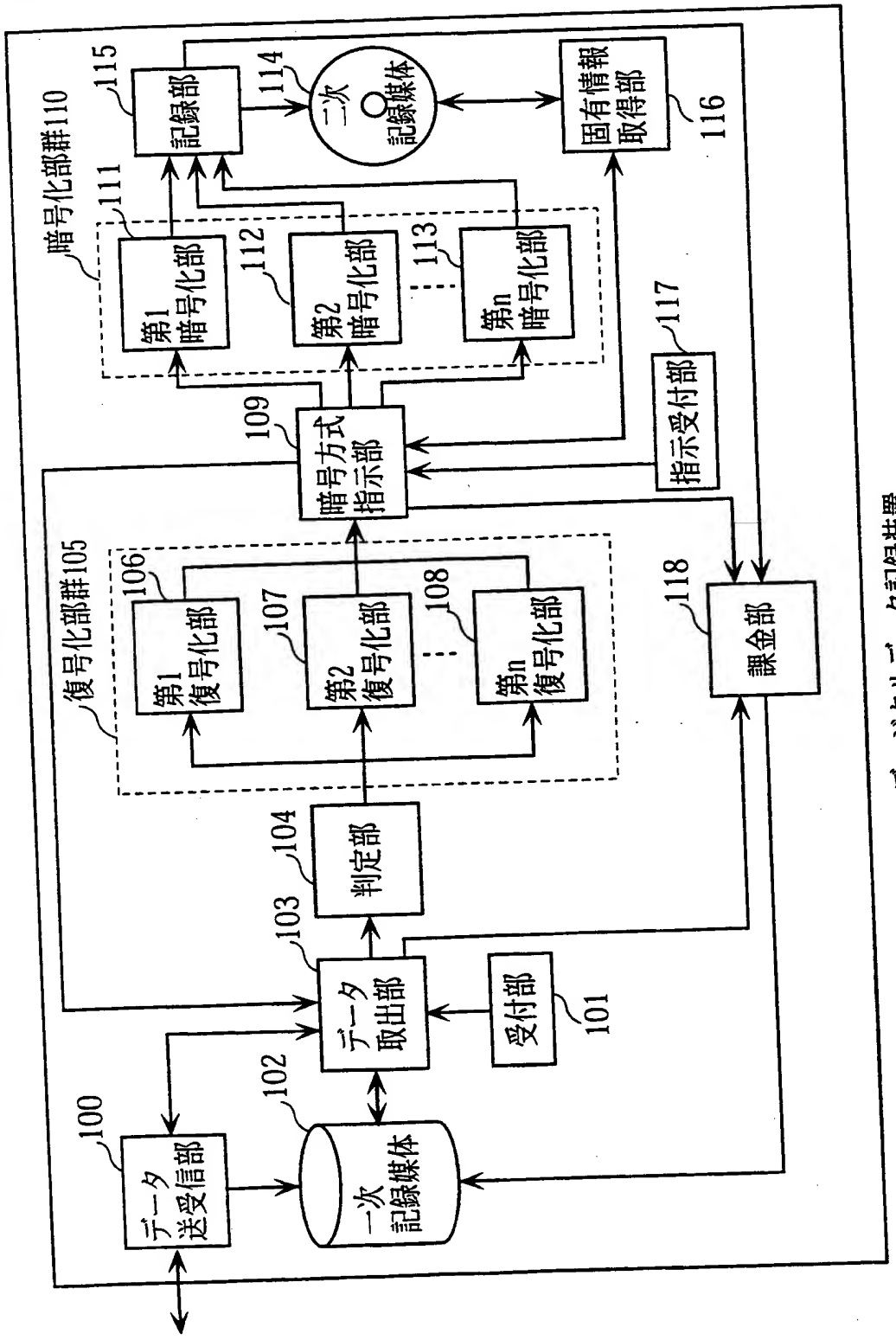

ディジタルデータ記録装置
データ送受信部
100
一次記録媒体
102
データ取出部
103
受付部
101
判定部
104
復号化部群105
第1復号化部
106
第2復号化部
107
第n復号化部
108
暗号方式指示部
109
暗号化部群110
第1暗号化部
111
第2暗号化部
112
第n暗号化部
113
記録部
115
二次記録媒体
114
固有情報取得部
116
指示受付部
117
課金部
118

図2

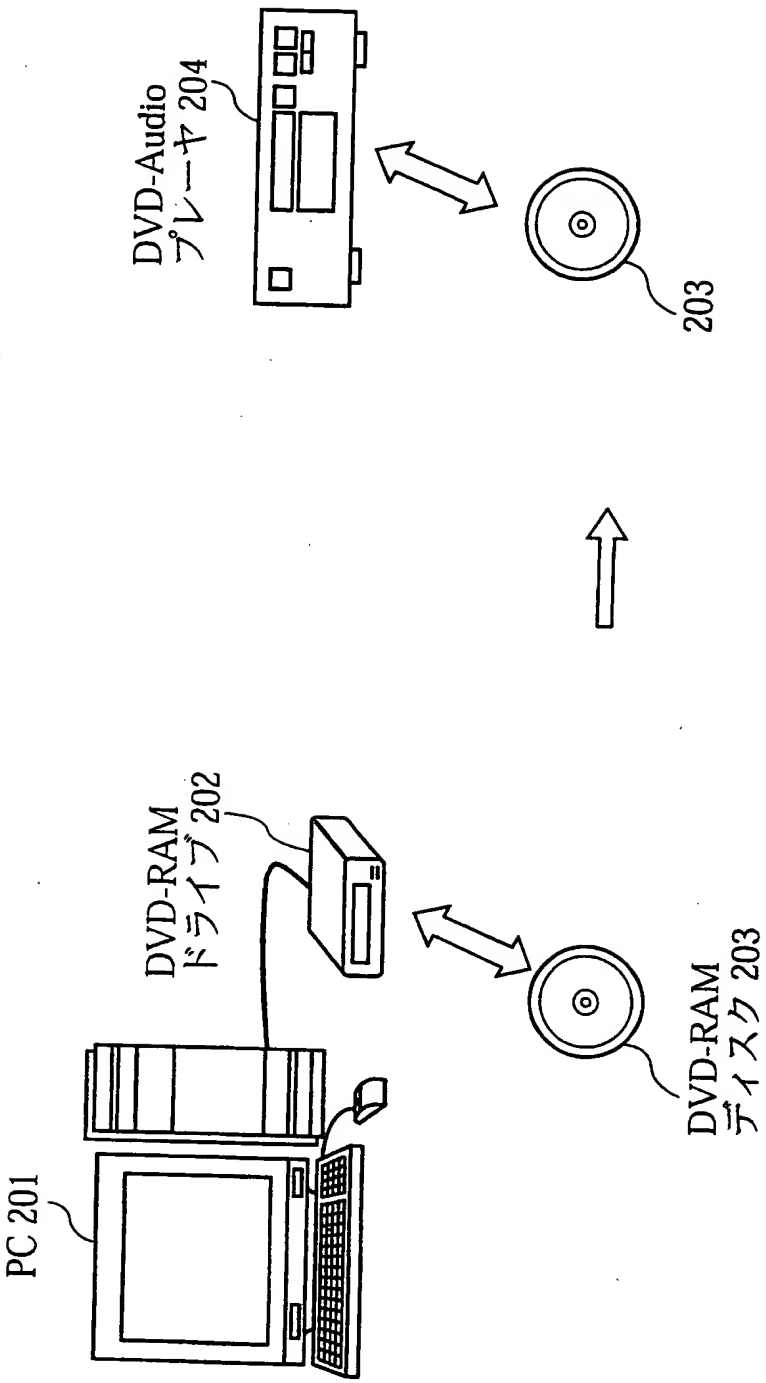


図3

301 曲名	302 歌手名	303 収録時間	304 価格
Song1	SingerA	4分20秒	100円
Song2	SingerB	3分53秒	50円
Song3	SingerC	4分48秒	75円
Song4	SingerD	4分06秒	100円
:	:	:	:
:	:	:	:

図4

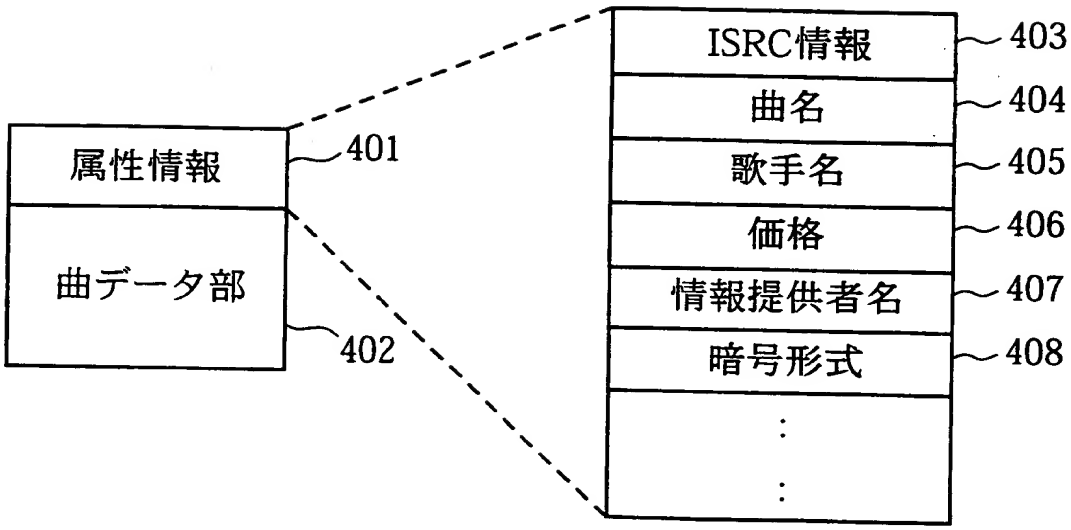

属性情報
401
曲データ部
402
ISRC情報
403
曲名
404
歌手名
405
価格
406
情報提供者名
407
暗号形式
408

図5

301 曲名	302 歌手名	303 収録時間	501 価格(1)	502 価格(2)
Song1	SingerA	4分20秒	100円	70円
Song2	SingerB	3分53秒	50円	35円
Song3	SingerC	4分48秒	75円	50円
Song4	SingerD	4分06秒	100円	100円
:	:	:	:	:
:	:	:	:	:

図6

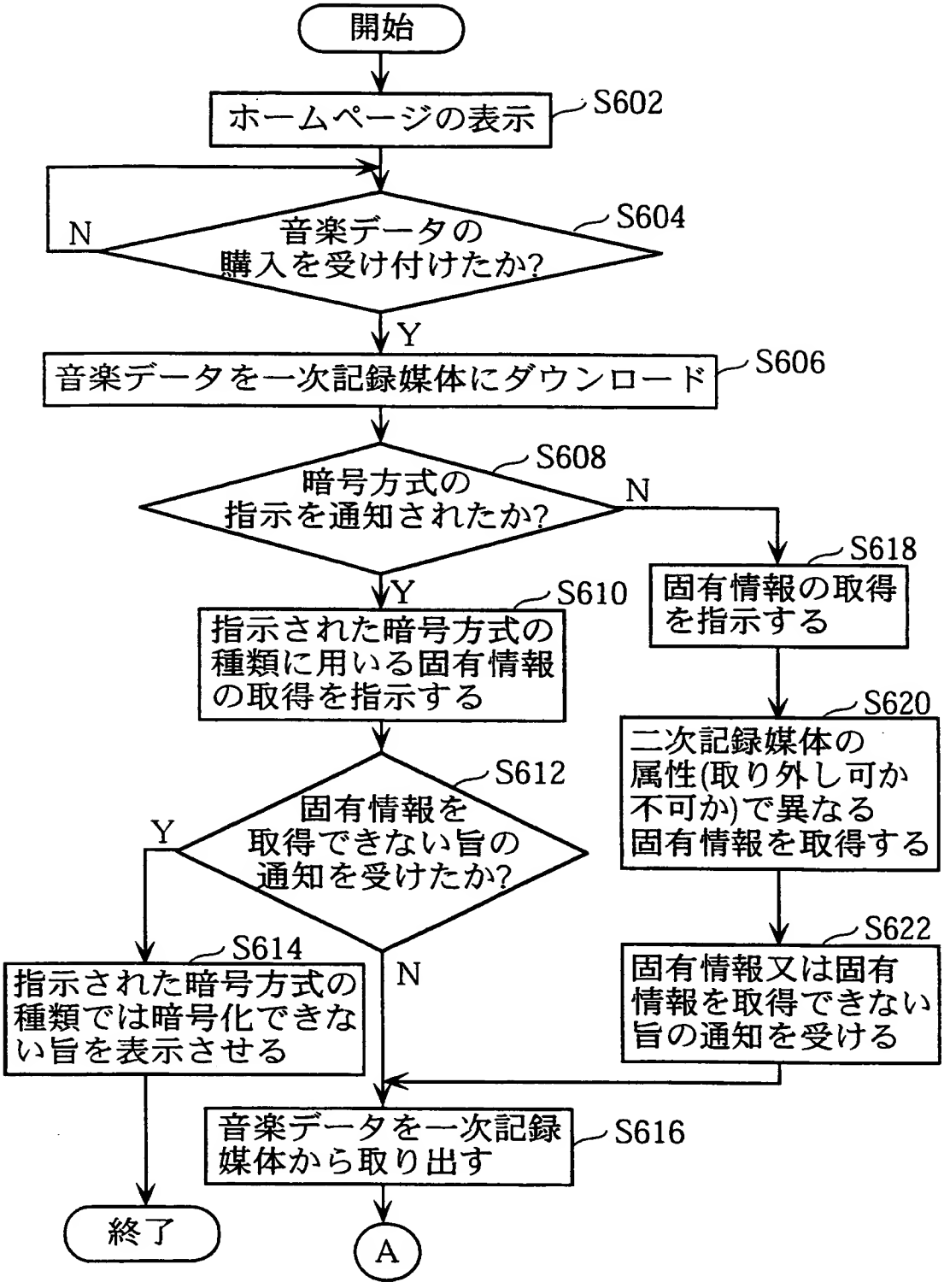

開始
ホームページの表示
S602
音楽データの購入を受け付けたか?
S604
N
Y
音楽データを一次記録媒体にダウンロード
S606
暗号方式の指示を通知されたか?
S608
N
Y
S610
指示された暗号方式の種類に用いる固有情報の取得を指示する
S612
固有情報を取得できない旨の通知を受けたか?
Y
N
S614
指示された暗号方式の種類では暗号化できない旨を表示させる
S618
固有情報の取得を指示する
S620
二次記録媒体の属性(取り外し可か不可か)で異なる固有情報を取得する
S622
固有情報又は固有情報を取得できない旨の通知を受ける
音楽データを一次記録媒体から取り出す
S616
終了
A

図7

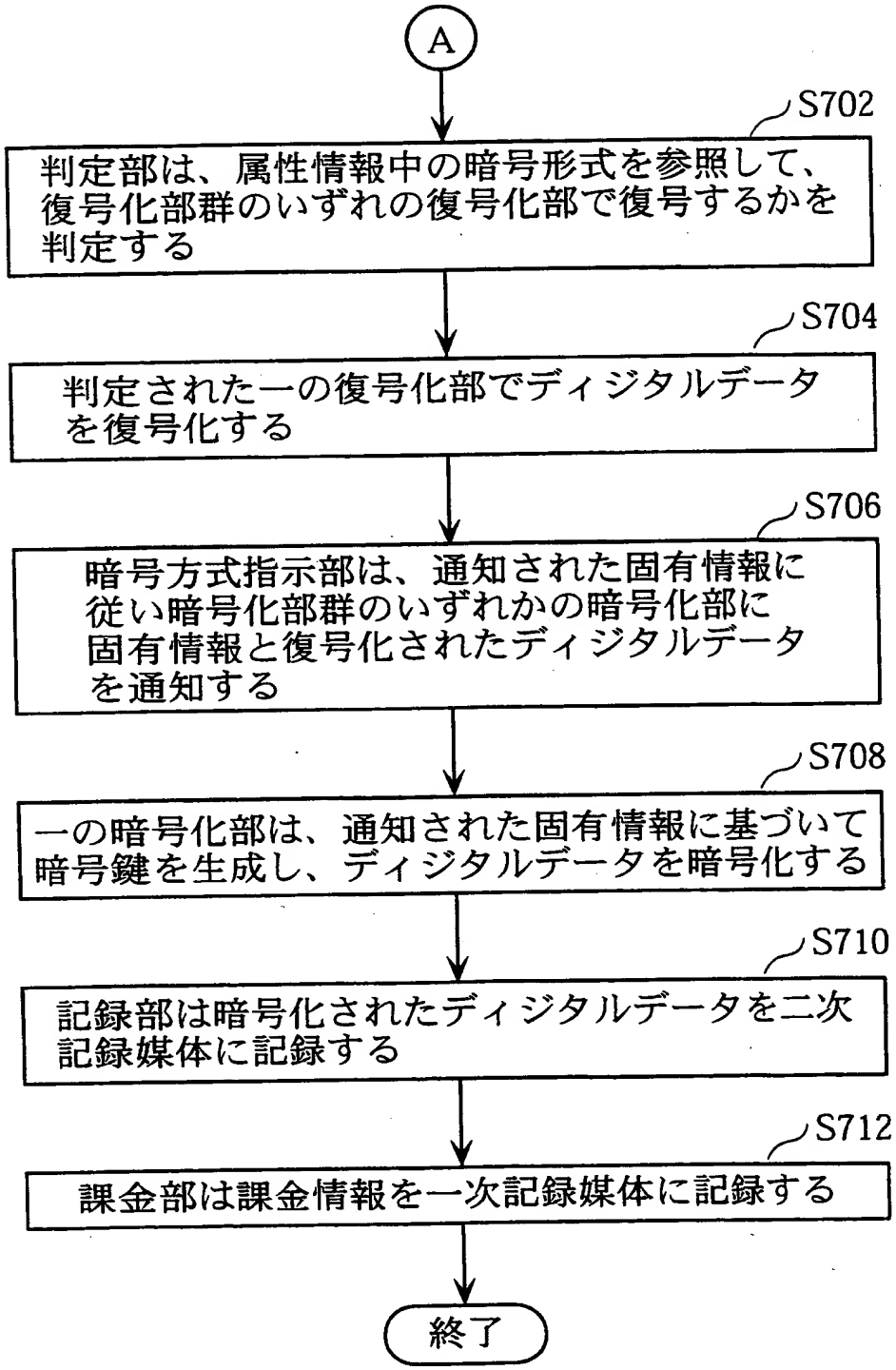

A
S702
判定部は、属性情報中の暗号形式を参照して、復号化部群のいずれの復号化部で復号するかを判定する
S704
判定された一の復号化部でディジタルデータを復号化する
S706
暗号方式指示部は、通知された固有情報に従い暗号化部群のいずれかの暗号化部に固有情報と復号化されたディジタルデータを通知する
S708
一の暗号化部は、通知された固有情報に基づいて暗号鍵を生成し、ディジタルデータを暗号化する
S710
記録部は暗号化されたディジタルデータを二次記録媒体に記録する
S712
課金部は課金情報を一次記録媒体に記録する
終了

図8

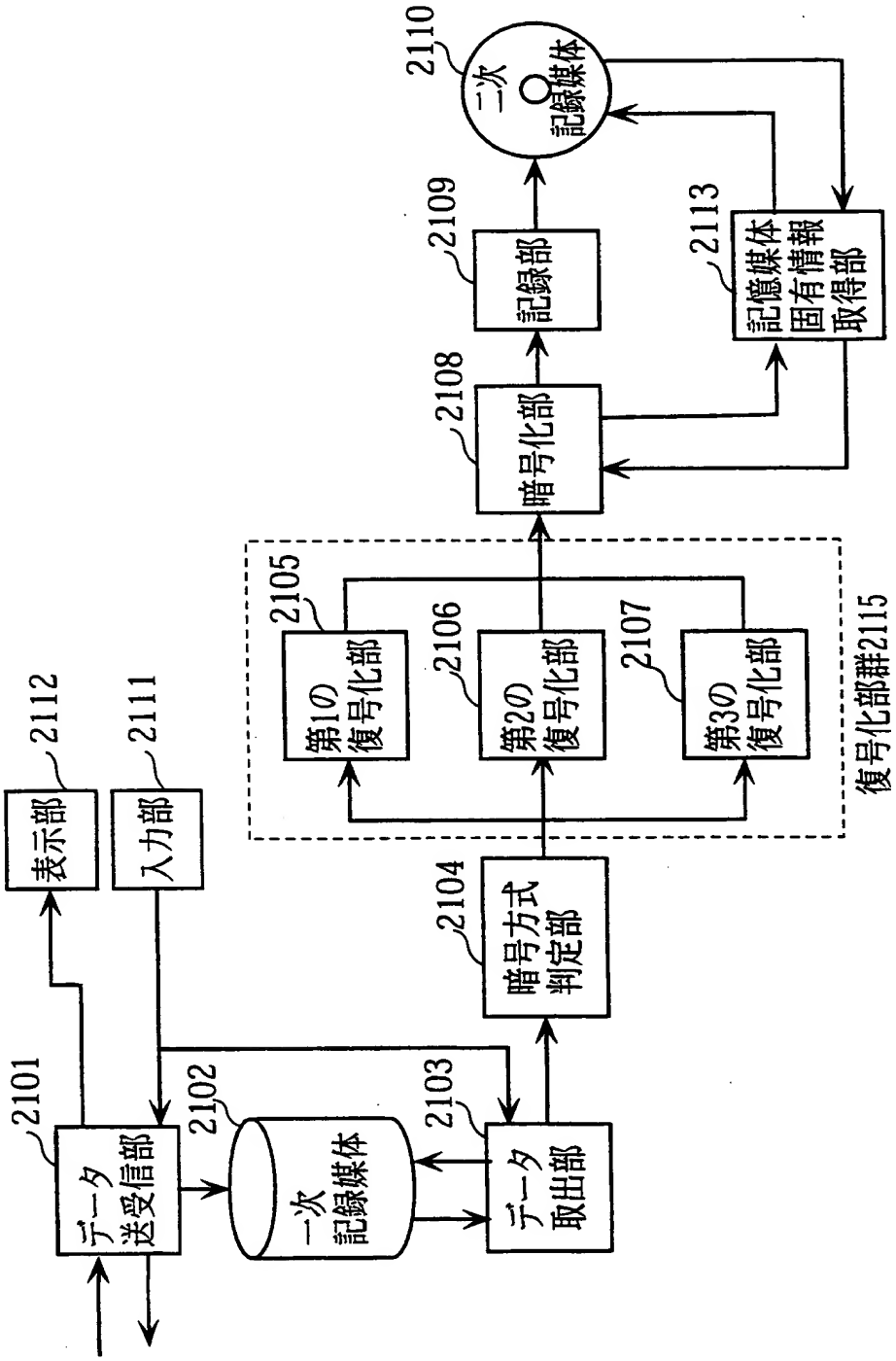

2110
二次記録媒体
2109
記録部
2113
記憶媒体固有情報取得部
2108
暗号化部
2105
第1の復号化部
2106
第2の復号化部
2107
第3の復号化部
復号化部群2115
2112
表示部
2111
入力部
2104
暗号方式判定部
2101
データ送受信部
2102
一次記録媒体
2103
データ取出部

図9

2201 曲名	2202 曲名コード	2203 歌手名	2204 データ入手先
曲A	song01	A	www. song/song01
曲B	song02	B	www. song/song02
曲C	song03	C	www. song/song03
曲D	song04	D	www. song/song04
曲E	song05	E	www. song/song05

図10

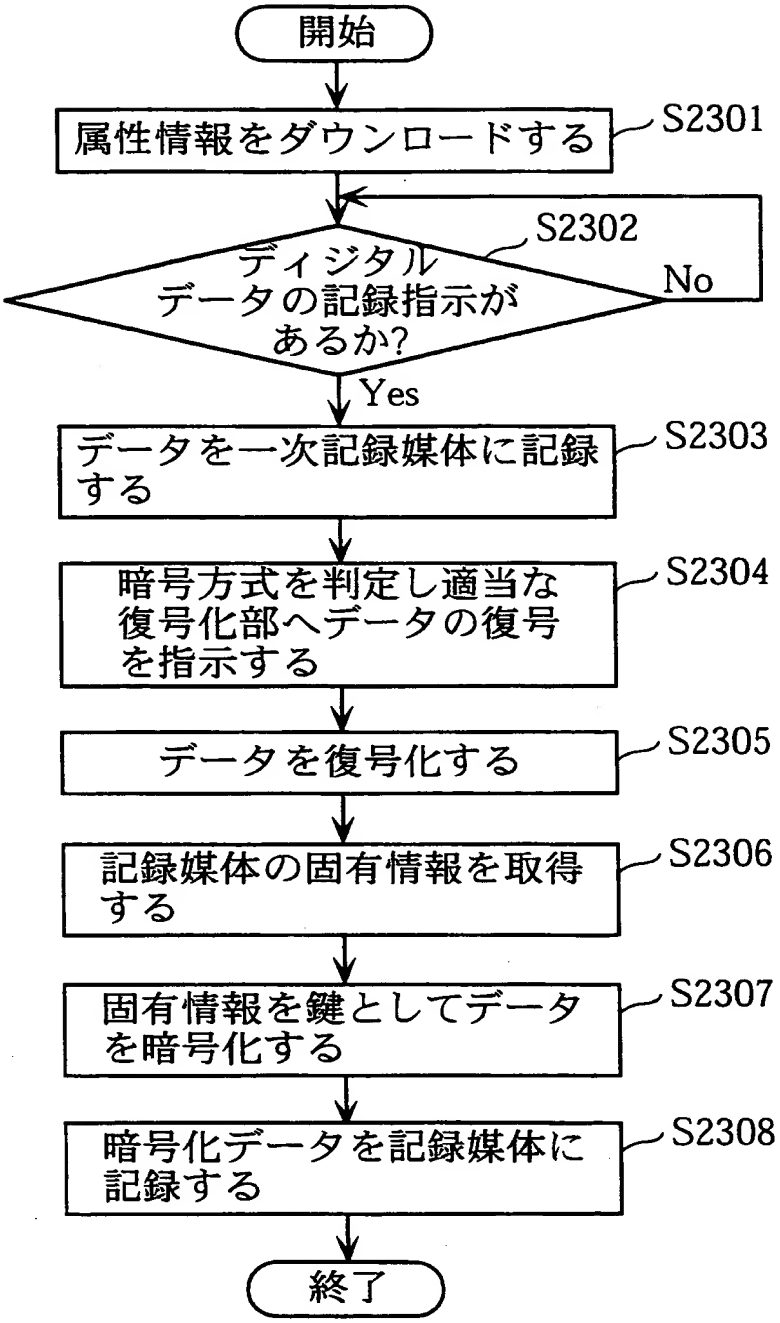

開始
属性情報をダウンロードする
S2301
ディジタルデータの記録指示があるか?
S2302
No
Yes
データを一次記録媒体に記録する
S2303
暗号方式を判定し適当な復号化部へデータの復号を指示する
S2304
データを復号化する
S2305
記録媒体の固有情報を取得する
S2306
固有情報を鍵としてデータを暗号化する
S2307
暗号化データを記録媒体に記録する
S2308
終了

図11

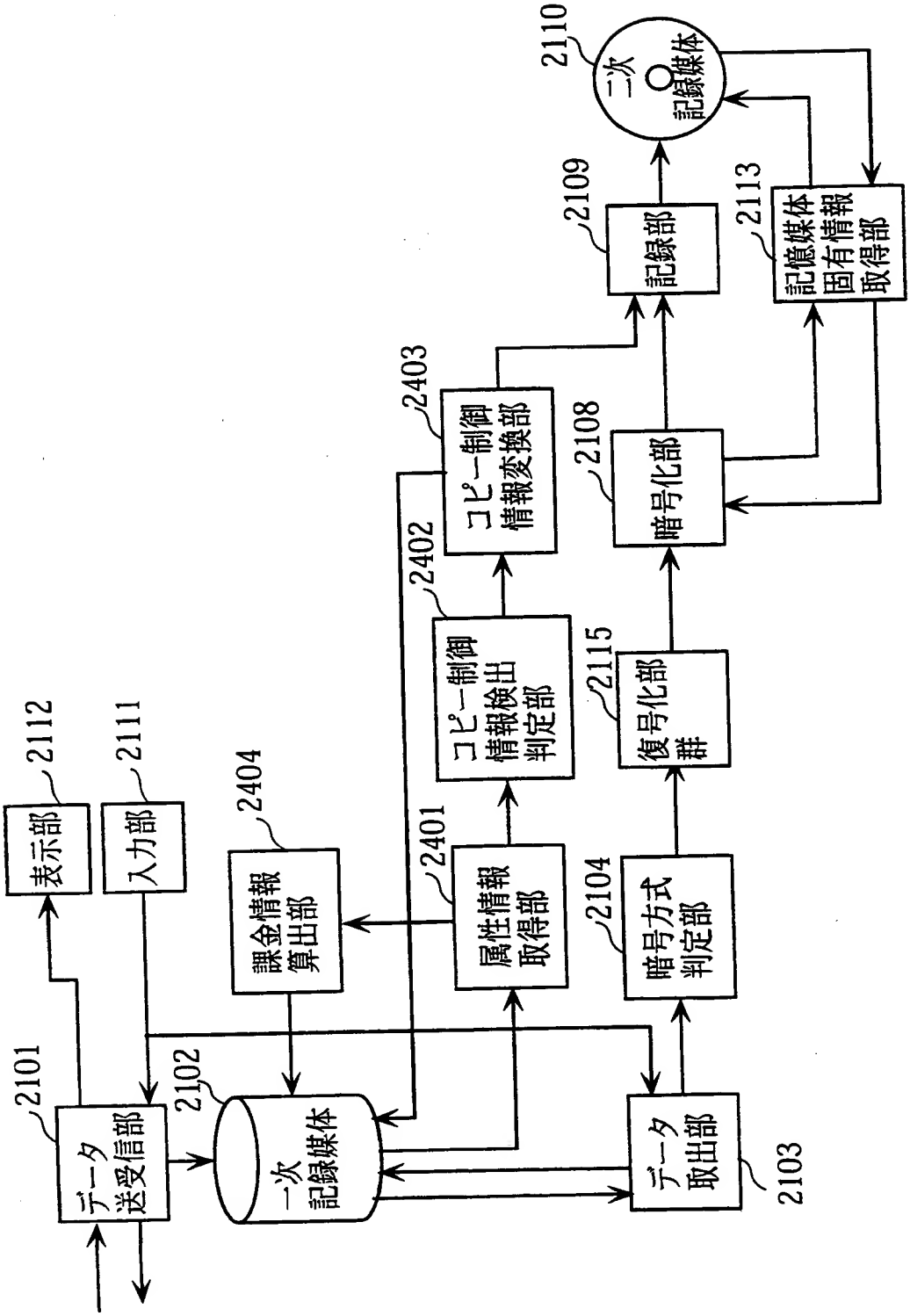
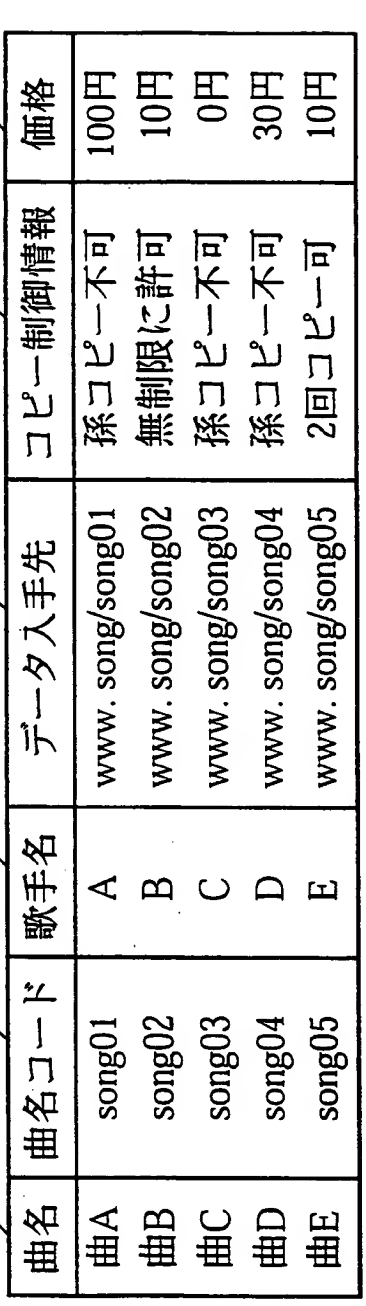

2110
二次
記録媒体
2109
記録部
2113
記憶媒体
固有情報
取得部
2403
コピー制御
情報変換部
2108
暗号化部
2402
コピー制御
情報検出
判定部
2115
復号化部
群
2112
表示部
2111
入力部
2404
課金情報
算出部
2401
属性情報
取得部
2104
暗号方式
判定部
2101
データ
送受信部
2102
一次
記録媒体
データ
取出部
2103

図12



曲名 (2201)	曲名コード (2202)	歌手名 (2203)	データ入手先 (2204)	コピー制御情報 (2501)	価格 (2502)
曲A	song01	A	www.song/song01	孫コピー不可	100円
曲B	song02	B	www.song/song02	無制限に許可	10円
曲C	song03	C	www.song/song03	孫コピー不可	0円
曲D	song04	D	www.song/song04	孫コピー不可	30円
曲E	song05	E	www.song/song05	2回コピー可	10円

図13

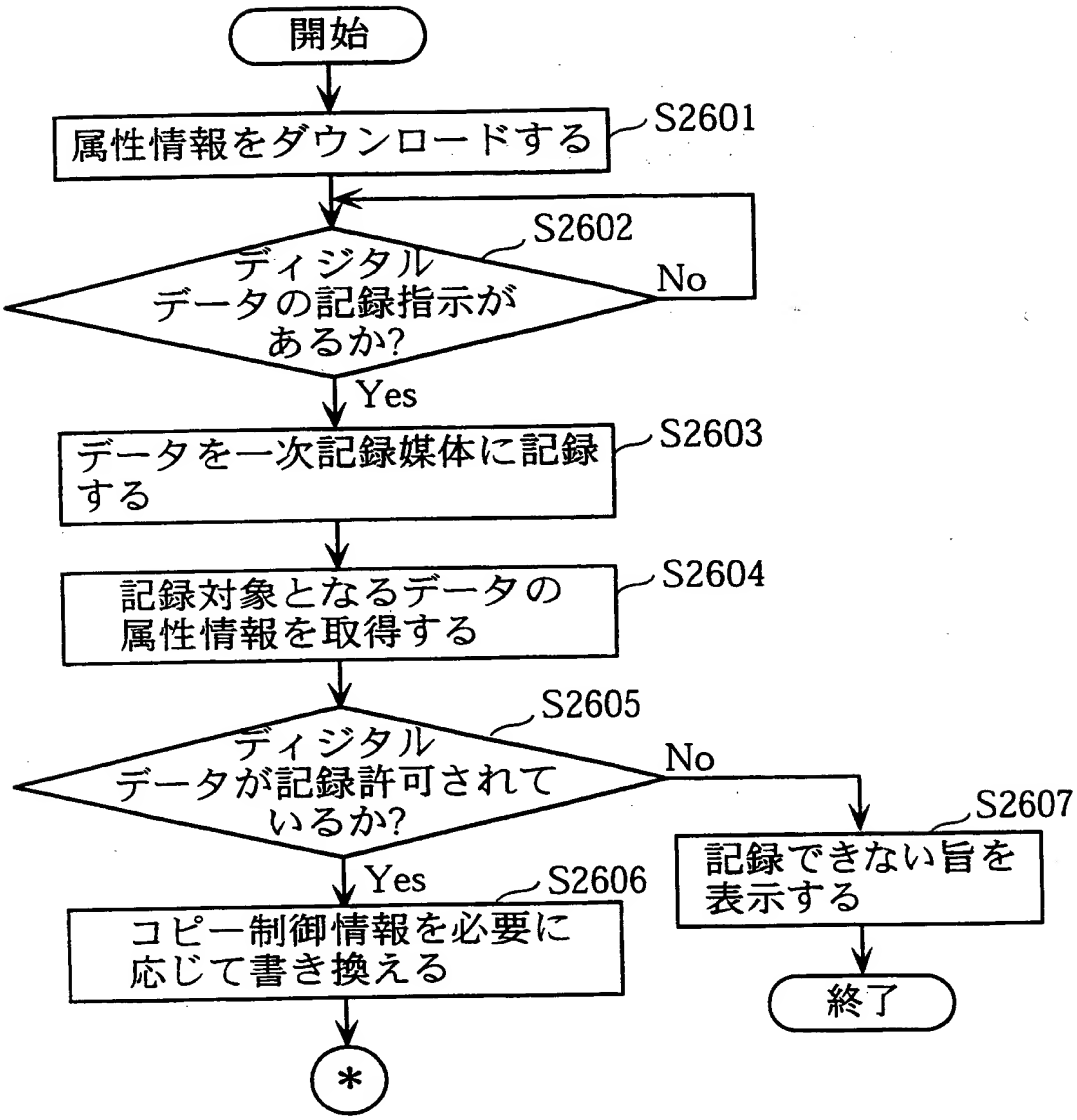

開始
属性情報をダウンロードする
S2601
S2602
ディジタル
データの記録指示が
あるか?
No
Yes
データを一次記録媒体に記録
する
S2603
記録対象となるデータの
属性情報を取得する
S2604
S2605
ディジタル
データが記録許可されて
いるか?
No
S2607
記録できない旨を
表示する
Yes
S2606
コピー制御情報を必要に
応じて書き換える
終了
*

図14

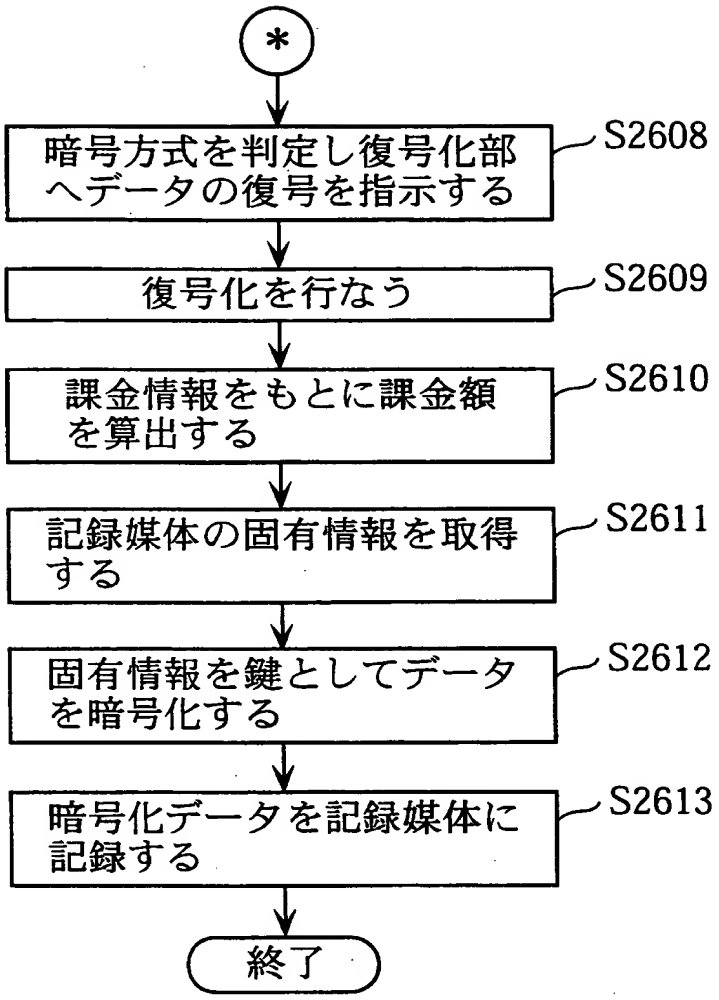


図15

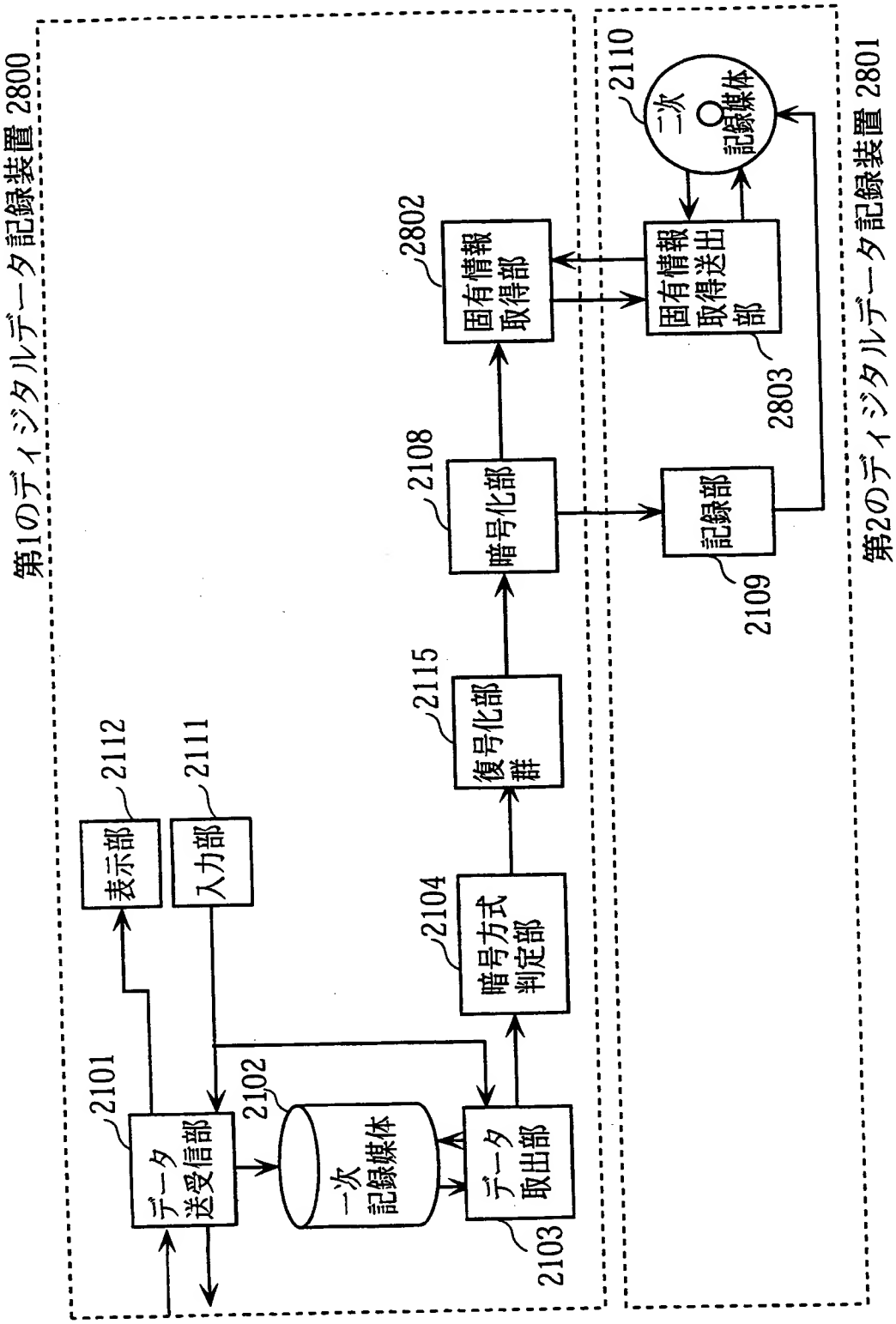

第1のディジタルデータ記録装置 2800
第2のディジタルデータ記録装置 2801
2101
データ送受信部
2102
一次記録媒体
2103
データ取出部
2104
暗号方式判定部
2108
暗号化部
2109
記録部
2110
二次記録媒体
2111
入力部
2112
表示部
2115
復号化部群
2802
固有情報取得部
2803
固有情報送出部

図16

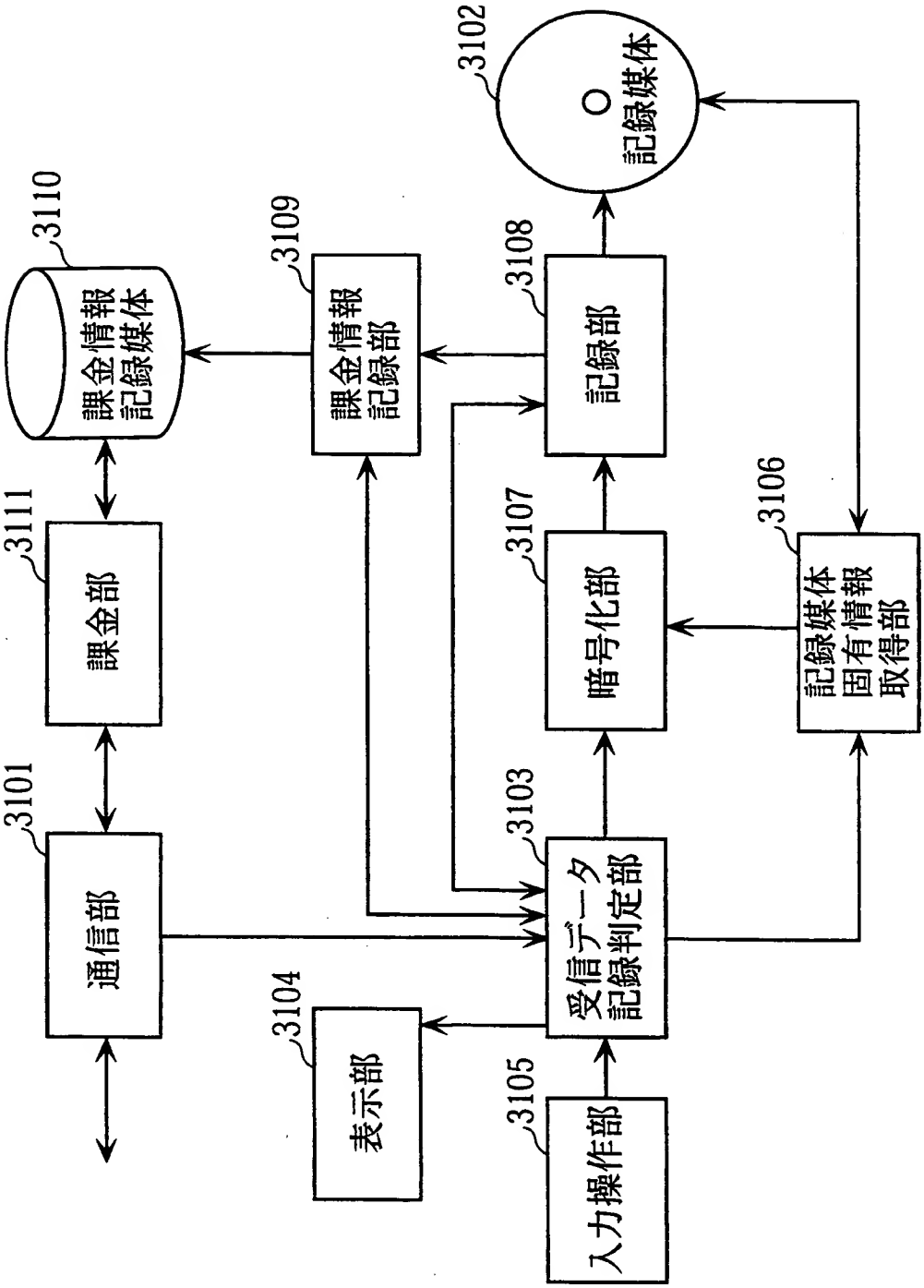


図17

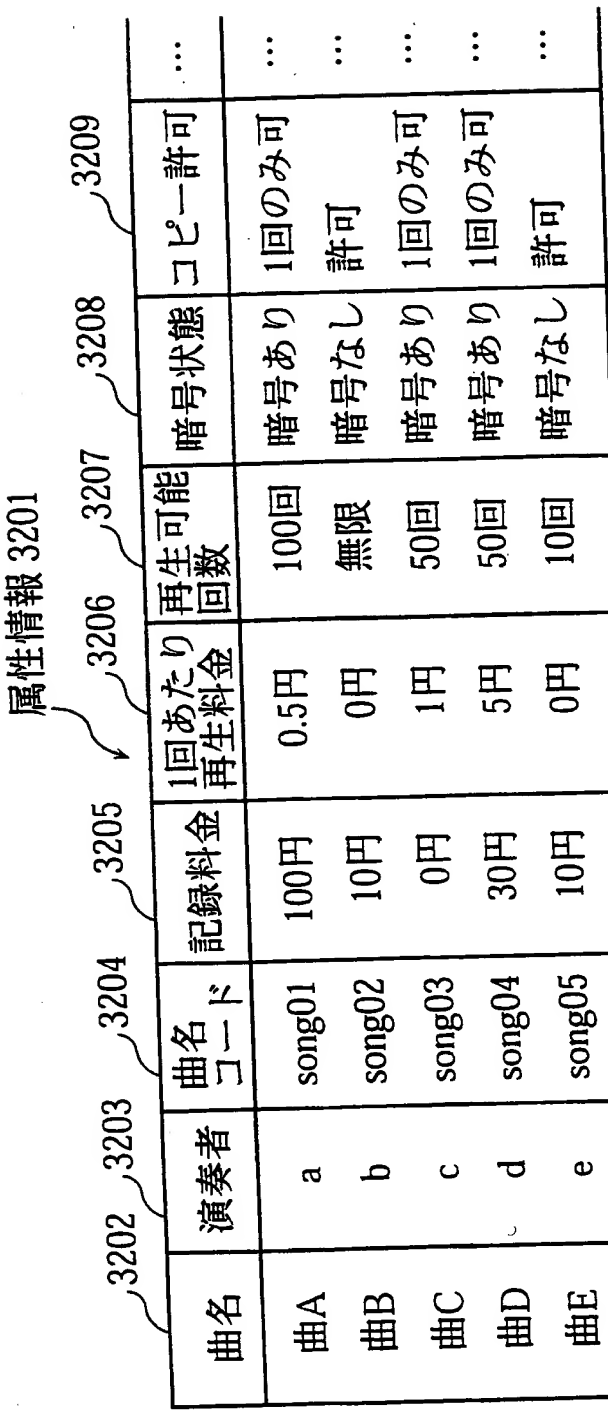

属性情報 3201
3202
3203
3204
3205
3206
3207
3208
3209
曲名
演奏者
曲名コード
記録料金
1回あたり再生料金
再生可能回数
暗号状態
コピー許可
曲A a song01 100円 0.5円 100回 暗号あり 1回のみ可 …
曲B b song02 10円 0円 無限 暗号なし 許可 …
曲C c song03 0円 1円 50回 暗号あり 1回のみ可 …
曲D d song04 30円 5円 50回 暗号あり 1回のみ可 …
曲E e song05 10円 0円 10回 暗号なし 許可 …

図18

管理情報 3301

3204 曲名コード	3302 記録開始アドレス	3303 記録終了アドレス
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

図19

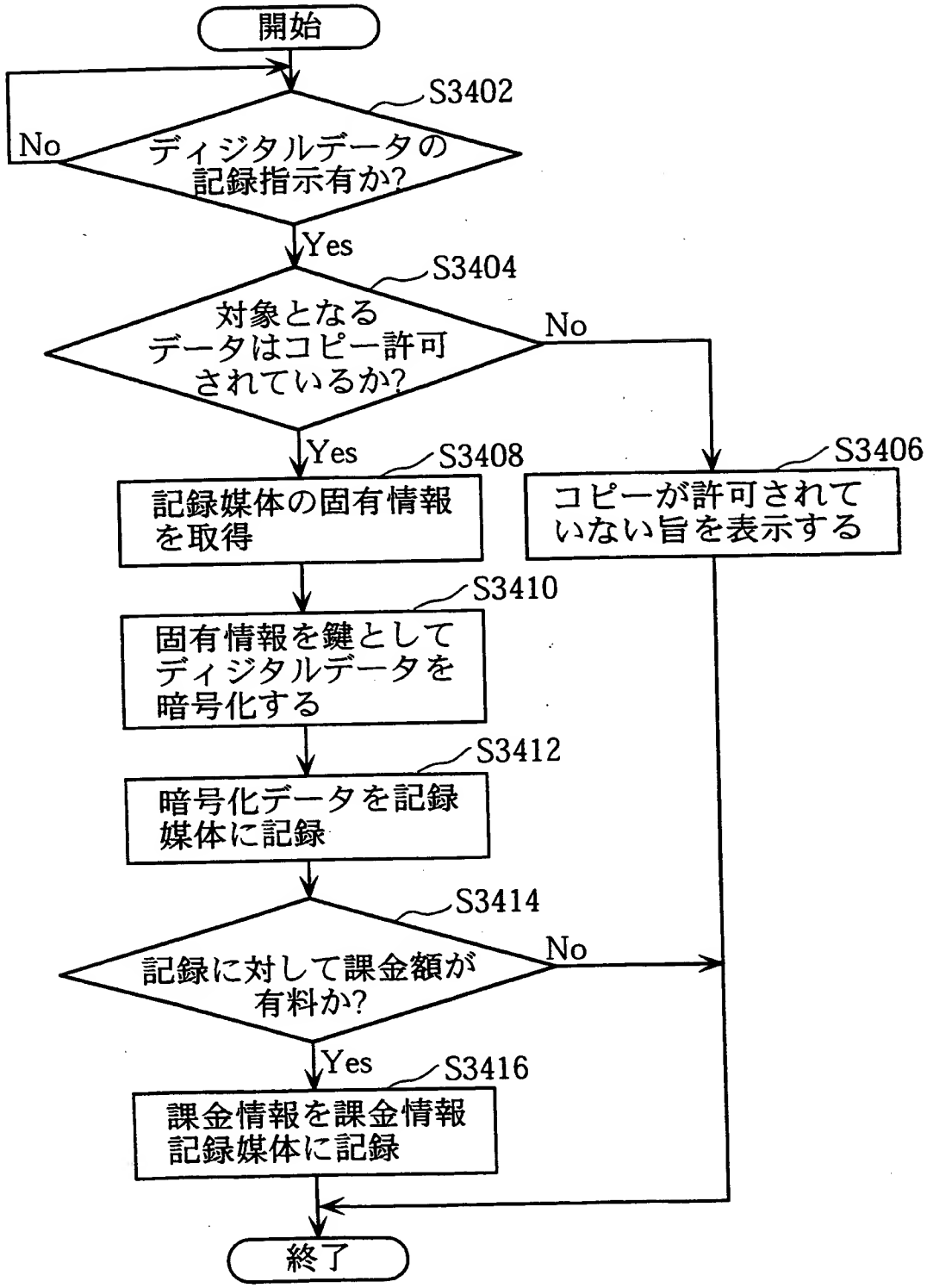

開始
S3402
No
ディジタルデータの記録指示有か?
Yes
S3404
対象となるデータはコピー許可されているか?
No
Yes
S3408
記録媒体の固有情報を取得
S3406
コピーが許可されていない旨を表示する
S3410
固有情報を鍵としてディジタルデータを暗号化する
S3412
暗号化データを記録媒体に記録
S3414
記録に対して課金額が有料か?
No
Yes
S3416
課金情報を課金情報記録媒体に記録
終了

図20

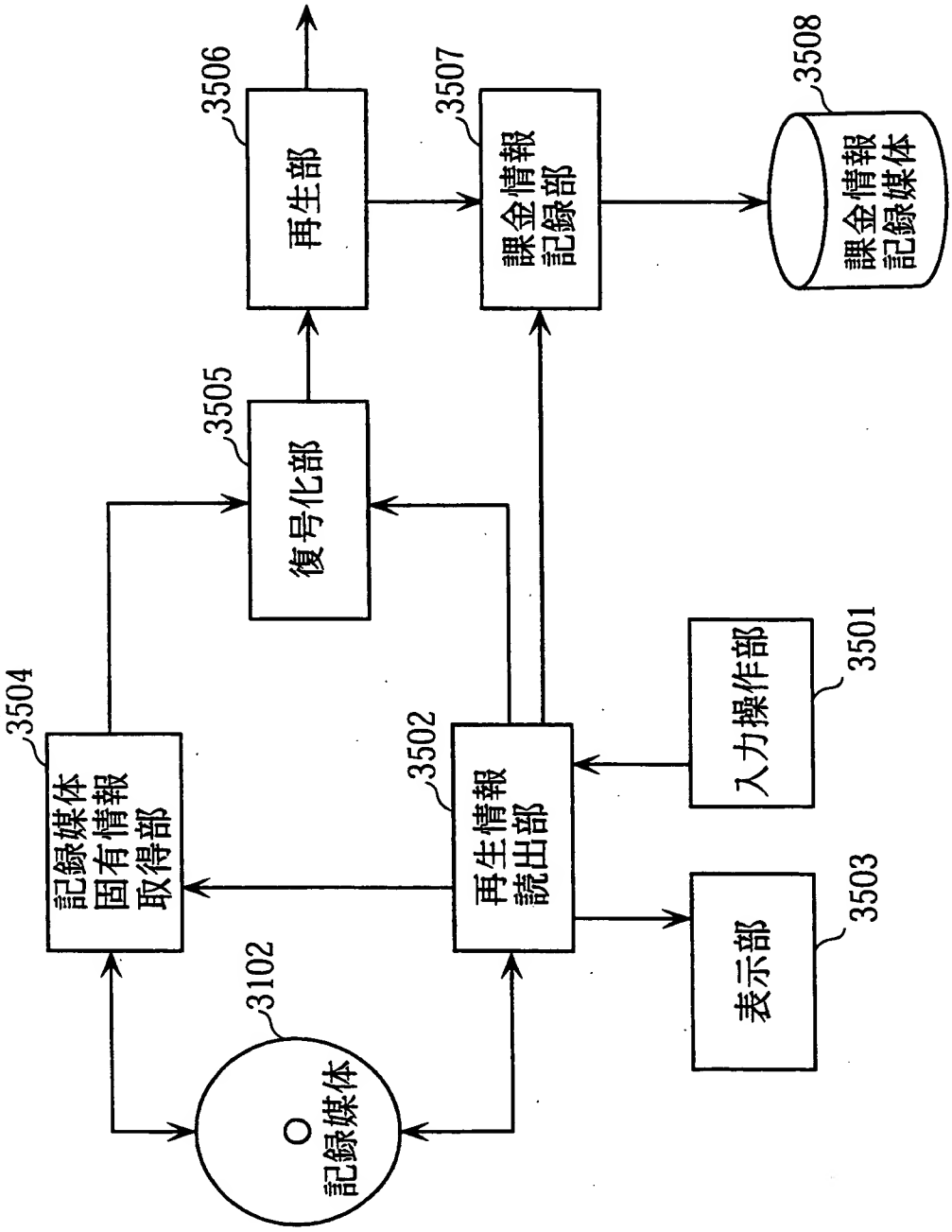


図21

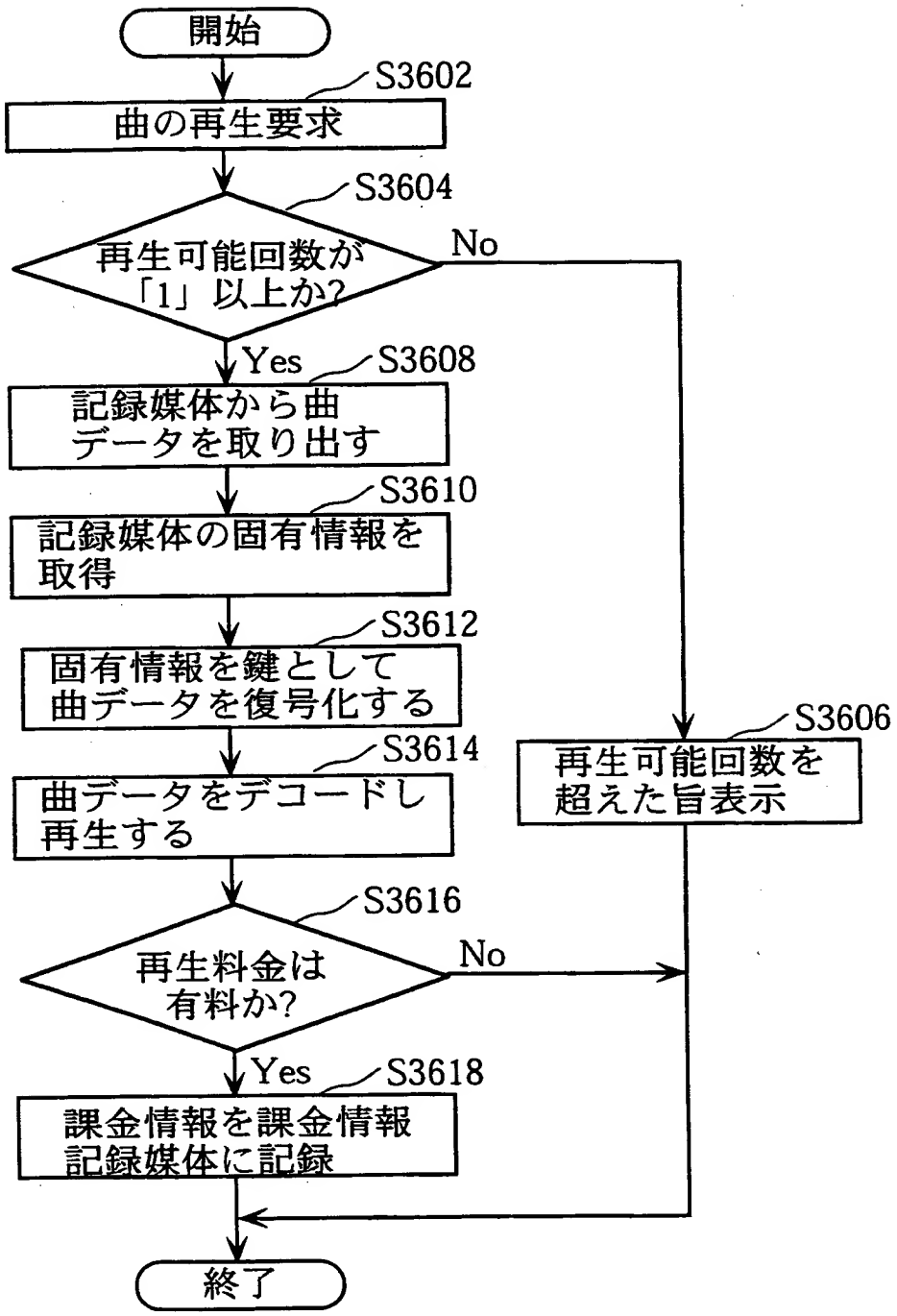

開始
S3602
曲の再生要求
S3604
再生可能回数が「1」以上か?
No
Yes
S3608
記録媒体から曲データを取り出す
S3610
記録媒体の固有情報を取得
S3612
固有情報を鍵として曲データを復号化する
S3614
曲データをデコードし再生する
S3606
再生可能回数を超えた旨表示
S3616
再生料金は有料か?
No
Yes
S3618
課金情報を課金情報記録媒体に記録
終了

図22

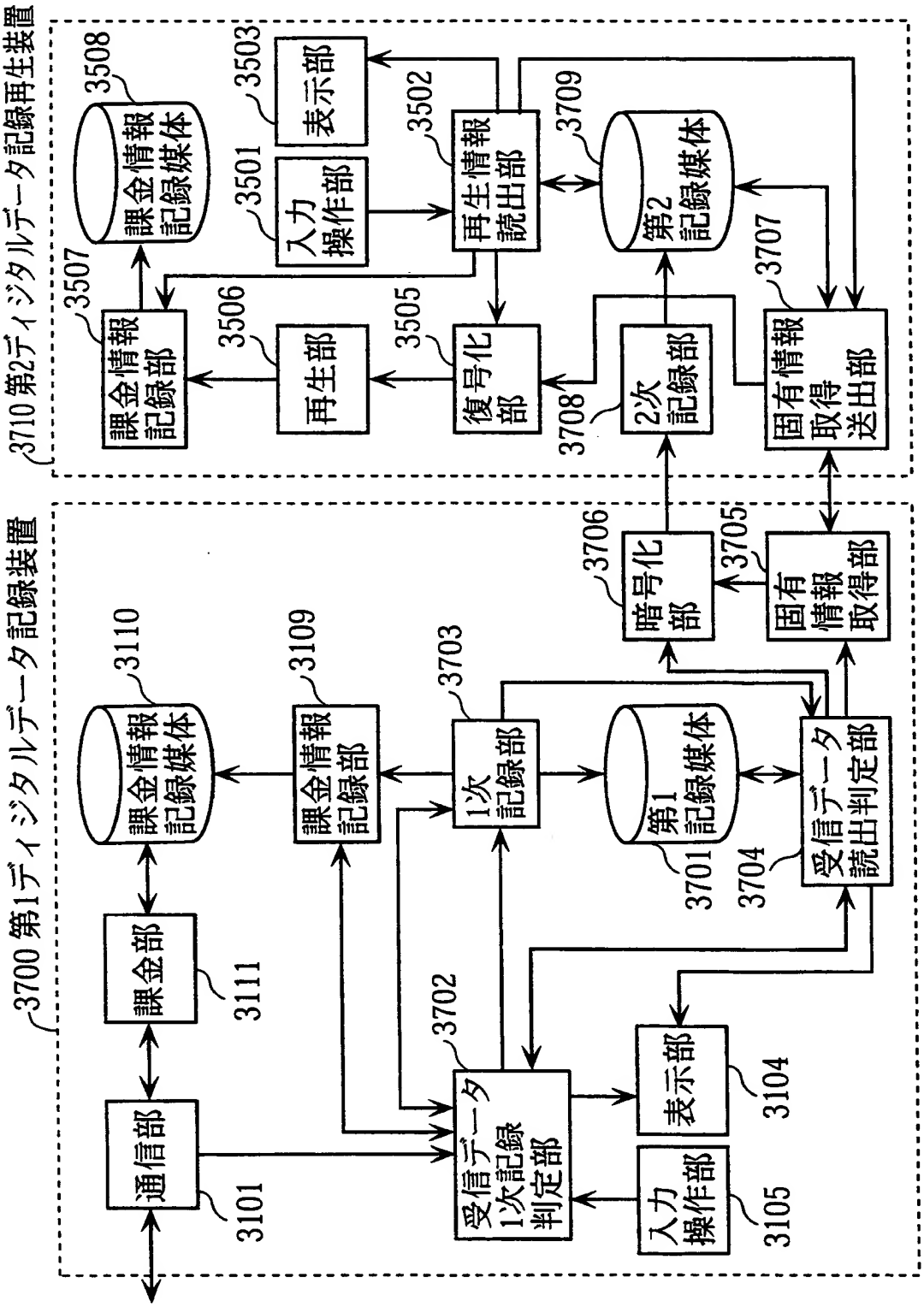
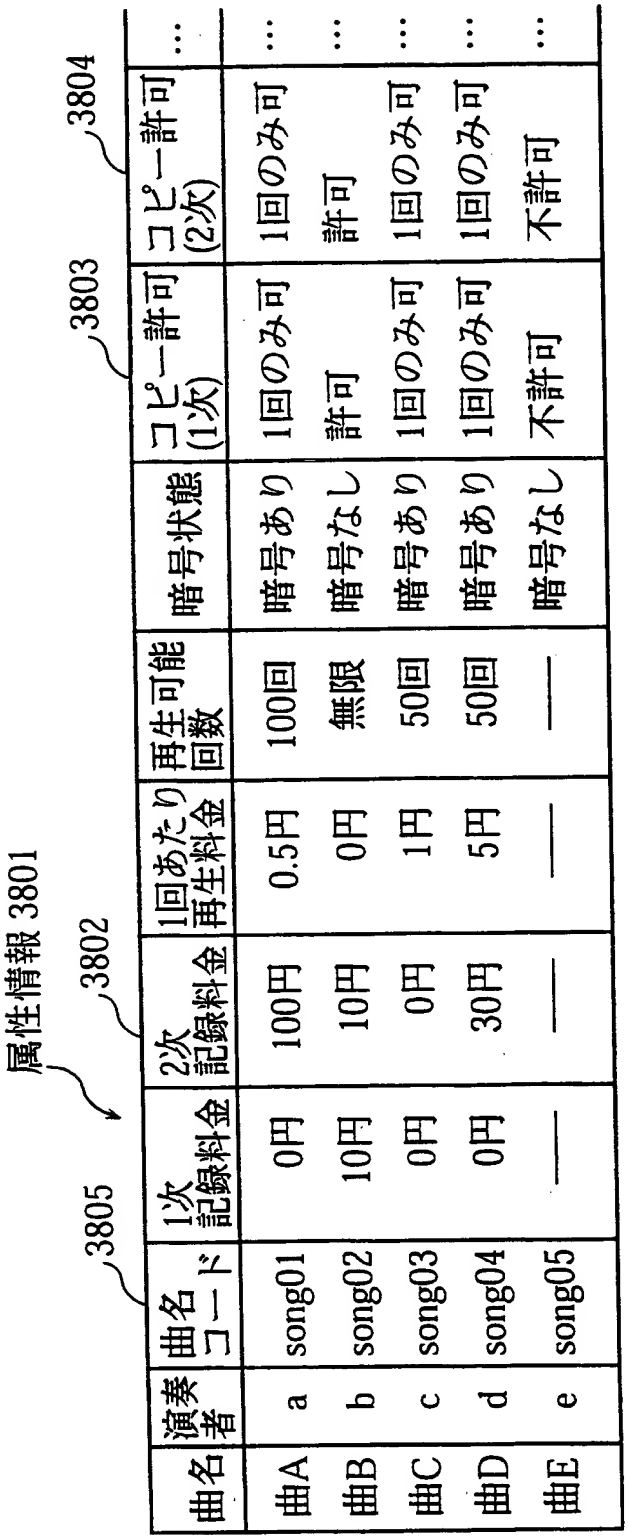

3700 第1ディジタルデータ記録装置
3710 第2ディジタルデータ記録再生装置
通信部
3101
課金部
3111
課金情報記録媒体
3110
課金情報記録部
3109
1次記録部
3703
第1記録媒体
3701
受信データ読出判定部
3704
暗号化部
3706
固有情報取得部
3705
受信データ1次記録判定部
3702
表示部
3104
入力操作部
3105
課金情報記録媒体
3508
課金情報記録部
3507
再生部
3506
復号化部
3505
2次記録部
3708
第2記録媒体
3709
固有情報取得送出部
3707
再生情報読出部
3502
入力操作部
3501
表示部
3503

図23



曲名	演奏者	曲名コード	1次記録料金	2次記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可(1次)	コピー許可(2次)	…
曲A	a	song01	0円	100円	0.5円	100回	暗号あり	1回のみ可	1回のみ可	…
曲B	b	song02	10円	10円	0円	無限	暗号なし	許可	許可	…
曲C	c	song03	0円	0円	1円	50回	暗号あり	1回のみ可	1回のみ可	…
曲D	d	song04	0円	30円	5円	50回	暗号あり	1回のみ可	1回のみ可	…
曲E	e	song05	—	—	—	—	暗号なし	不許可	不許可	…

図24

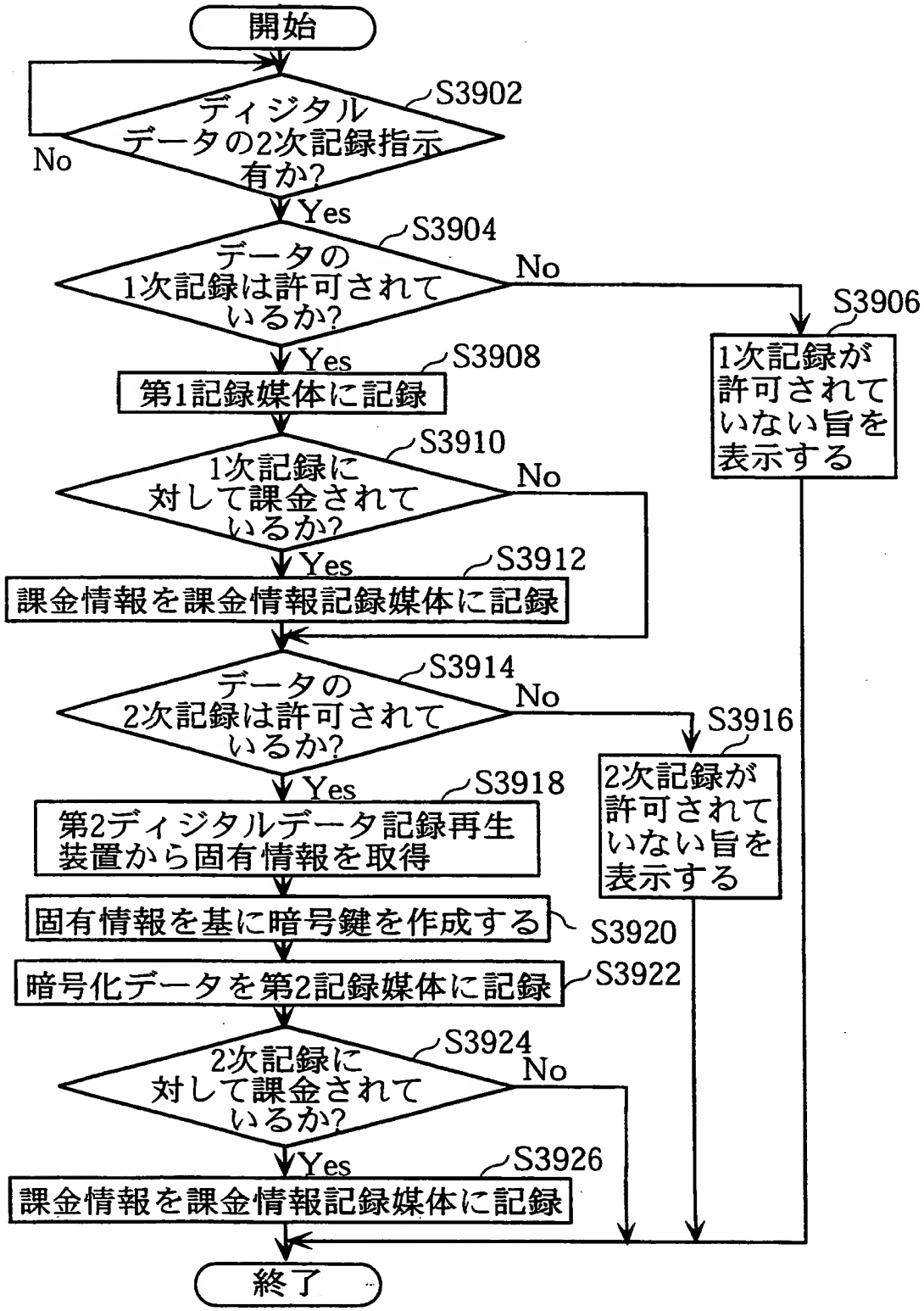
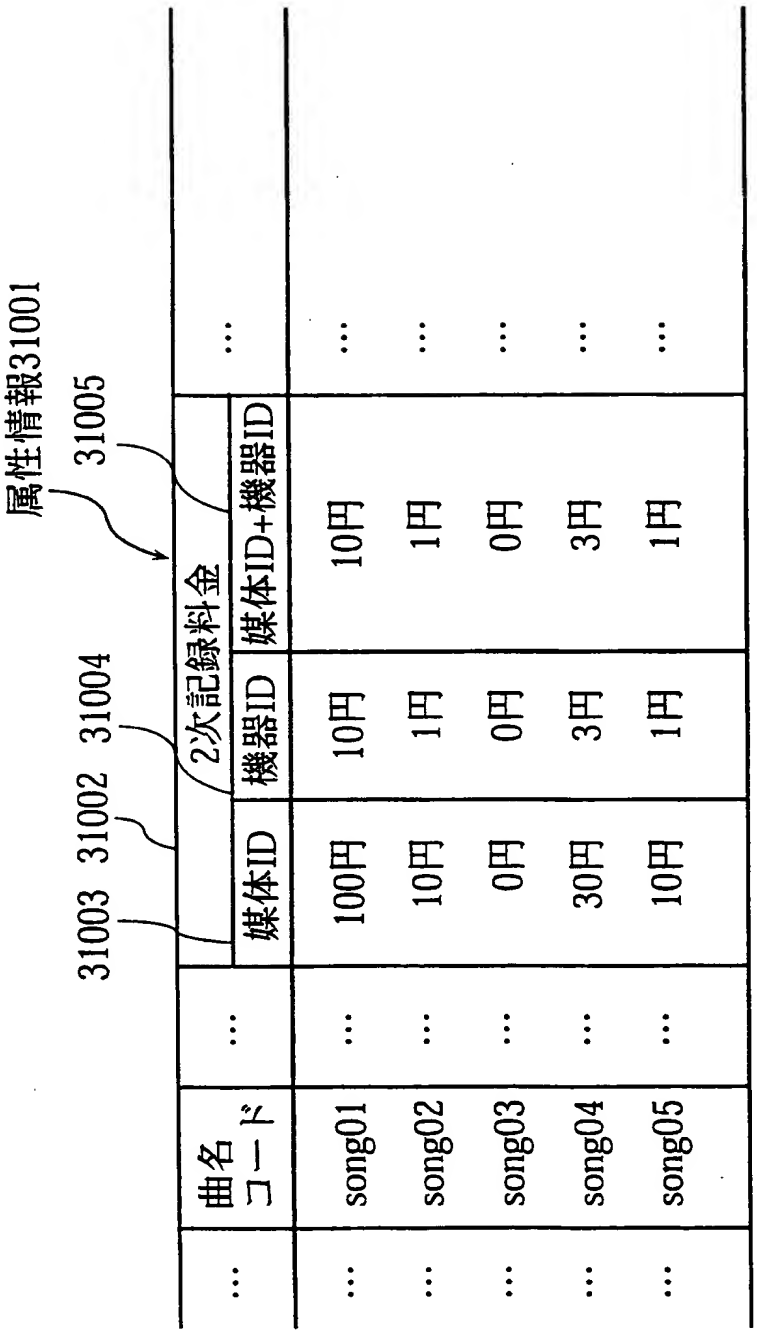

開始
ディジタルデータの2次記録指示有か?
S3902
No
Yes
データの1次記録は許可されているか?
S3904
No
S3906
1次記録が許可されていない旨を表示する
Yes
S3908
第1記録媒体に記録
1次記録に対して課金されているか?
S3910
No
Yes
S3912
課金情報を課金情報記録媒体に記録
データの2次記録は許可されているか?
S3914
No
S3916
2次記録が許可されていない旨を表示する
Yes
S3918
第2ディジタルデータ記録再生装置から固有情報を取得
固有情報を基に暗号鍵を作成する
S3920
暗号化データを第2記録媒体に記録
S3922
2次記録に対して課金されているか?
S3924
No
Yes
S3926
課金情報を課金情報記録媒体に記録
終了

図25


属性情報31001
31005
31004
31002
31003
2次記録料金
曲名コード
媒体ID
機器ID
媒体ID+機器ID
song01 100円 10円 10円
song02 10円 1円 1円
song03 0円 0円 0円
song04 30円 3円 3円
song05 10円 1円 1円

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/03887

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1999 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-272399, A (Hitachi,Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 & US, 5912969, A	1-12
A	JP, 8-339629, A (Matsushita Electric Industrial Co., Ltd.), 24 December, 1996 (24. 12. 96), Full text ; Figs. 1 to 4 (Family: none)	1-12
P, A	JP, 11-191266, A (Kobe Steel,Ltd.), 13 July, 1999 (13. 07. 99), Full text ; Figs. 1, 2 (Family: none)	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 October, 1999 (19. 10. 99)	2 November, 1999 (02. 11. 99)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０３８８７

A.　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ[6]　Ｇ１１Ｂ２０／１０

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Ｉｎｔ．Ｃｌ[6]　Ｇ１１Ｂ２０／１０

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　１９２２－１９９９年
日本国公開実用新案公報　１９７１－１９９９年
日本国登録実用新案公報　１９９４－１９９９年
日本国実用新案登録公報　１９９６－１９９９年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ，７－２７２３９９，Ａ（株式会社日立製作所） ２０．１０月．１９９５（２０．１０．９５） 全文，第１－１８図 ＆　ＵＳ，５９１２９６９，Ａ	１－１２
Ａ	ＪＰ，８－３３９６２９，Ａ（松下電器産業株式会社） ２４．１２月．１９９６（２４．１２．９６） 全文，第１－４図（ファミリーなし）	１－１２
Ｐ，Ａ	ＪＰ，１１－１９１２６６，Ａ（株式会社神戸製鋼所） １３．７月．１９９９（１３．０７．９９） 全文，第１－２図（ファミリーなし）	１－１２

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日　１９．１０．９９

国際調査報告の発送日　02.11.99

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｑ　７７３６
小松　正　印

電話番号　０３－３５８１－１１０１　内線　６９２２

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）